Xử lý sự cố
an toàn thông tin

Mục lục

Chương 1: Giới thiệu về Xử lý sự cố

Cơ bản về bảo mật

Chu trình bảo mật thông tin

Để thành công và đáng tin cậy như một chuyên gia bảo mật, bạn cần hiểu bảo mật trong kinh doanh bắt đầu từ dưới lên. Bạn cũng nên biết những điều khoản và ý tưởng bảo mật chính sử dụng bởi các chuyên gia bảo mật khác trong tài liệu kỹ thuật và trong các ấn phẩm thương mại an ninh quan trọng. Triển khai bảo mật được xây dựng từ các khối xây dựng cơ bản, giống như một tòa nhà lớn được xây dựng từ từng viên gạch. Chủ đề này sẽ giúp bạn hiểu được những khối xây dựng để bạn có thể sử dụng chúng như là nền tảng cho sự nghiệp bảo mật của bạn.

Bảo mật thông tin là gì?

An ninh thông tin đề cập đến việc bảo vệ thông tin hoặc nguồn lực thông tin sẵn có khỏi những truy cập trái phép, tấn công, trộm cắp, hoặc hư hỏng dữ liệu. Các cá nhân và tổ chức có trách nhiệm phải bảo mật thông tin của họ. Do sự hiện diện của một môi trường kinh doanh kết nối rộng rãi, dữ liệu bây giờ sẵn sàng trong một loạt các hình thức như: phương tiện truyền thông kỹ thuật số và in ấn. Vì vậy, mỗi bit dữ liệu đang được sử dụng, chia sẻ, hoặc truyền phải được bảo vệ để giảm thiểu rủi ro kinh doanh và hậu quả khác của việc mất dữ liệu quan trọng.

Bảo vệ cái gì

Là một chuyên gia an ninh thông tin, bạn cần phải biết những thông tin nào cần bảo đảm trong một tổ chức và tại sao những tài sản cần được bảo vệ.

- Dữ liệu : Đây là một thuật ngữ chung liên quan đến các tài sản thông tin của một người, khách hàng, hoặc tổ chức. Trong một hệ thống máy tính, các tập tin dữ liệu. Bạn cần để bảo vệ dữ liệu khỏi bị hỏng hoặc bị truy cập mà không có phép.
- Tài nguyên : Đây là những thành phần hệ thống ảo hay vật lý có giới hạn tính sẵn sàng. Một nguồn lực vật lý là bất kỳ thiết bị kết nối trực tiếp đến một hệ thống máy tính. Một nguồn tài nguyên ảo dùng để chỉ các loại tập tin, vị trí bộ nhớ, hoặc kết nối mạng.

Mục tiêu của bảo mật

Có ba mục tiêu chính hoặc các chức năng liên quan đến việc thực hành bảo mật thông tin.

- Phòng ngừa
- Dò tìm
- Phục hồi

Rủi ro

Khi áp dụng cho các hệ thống thông tin, rủi ro là một khái niệm mà chỉ tiếp xúc với các nguy cơ hư hỏng hoặc mất mát. Nó thể hiện khả năng gây nguy hiểm hoặc đe dọa nguy hiểm xảy ra.

Mối đe dọa

Trong lĩnh vực bảo mật máy tính, một mối đe dọa là bất kỳ sự kiện hoặc hành động có tiềm năng có thể gây thiệt hại cho tài sản. Các mối đe dọa thường vi phạm các yêu cầu an ninh, chính sách hay thủ tục. Bất kể một sự vi phạm là cố ý hoặc vô ý, độc hại hay không, nó được coi là một mối đe dọa.

Lỗ hổng

Ở cấp độ cơ bản nhất, một lỗ hổng là bất kỳ điều kiện nào khiến một hệ thống bị gây hại.

Xâm nhập

Trong lĩnh vực bảo mật máy tính, một sự xâm nhập xảy ra khi một kẻ tấn công truy cập một hệ thống máy tính mà không được phép làm như vậy.

Tấn công

Trong lĩnh vực bảo mật máy tính, một cuộc tấn công là một kỹ thuật được sử dụng để khai thác một lỗ hổng trong bất kỳ ứng dụng hoặc hệ thống máy tính vật lý mà không được phép làm như vậy.

Kiểm soát

Trong lĩnh vực bảo mật máy tính, kiểm soát là các biện pháp đối phó mà bạn cần phải đưa ra để tránh, giảm thiểu, hoặc chống lại các rủi ro an ninh do các

mối đe dọa hoặc tấn công. Nói cách khác, các điều khiển là những giải pháp và hoạt động cho phép một tổ chức để đáp ứng các mục tiêu của chiến lược an ninh thông tin. Điều khiển có thể được bảo vệ và biện pháp đối phó đó là hợp lý hoặc thể chất. Điều khiển được phân loại như các điều khiển chỉnh phòng ngừa, phát hiện, và.

Quy trình quản lý anh ninh

Quy trình quản lý an ninh liên quan đến việc xác định, thực hiện, giám sát và kiểm soát an ninh.

Kiểm soát bảo mật thông tin

Bạn đã vừa xác định các thành phần của chu kỳ bảo mật thông tin. Bây giờ bạn có thể tìm hiểu làm thế nào mà họ kiểm soát an ninh máy tính. Trong chủ đề này, bạn sẽ xác định kiểm soát an ninh một cách chi tiết hơn và xác định làm thế nào điều khiển được thực hiện trong bảo mật máy tính.

Hiểu biết về các vấn đề cơ bản của chu kỳ bảo mật thông tin chỉ là bước đầu tiên trong việc khám phá làm thế nào những yếu tố kiểm soát an ninh máy tính như một toàn thể. Bằng cách xác định kiểm soát an ninh thông tin và làm thế nào các chuyên gia bảo mật khác sử dụng chúng trong lĩnh vực này, bạn sẽ được chuẩn bị tốt hơn để lựa chọn và thực hiện các điều khiển thích hợp tại nơi làm việc của riêng bạn.

Tam giác bảo mật CIA

Tam giác CIA bao gồm ba nguyên tắc.

Nguyên tắc	*Mô tả*
Bảo mật - Confidentiality	Đây là nguyên tắc cơ bản của việc giữ thông tin và truyền thông tin và bảo vệ họ khỏi những truy cập trái phép.
Toàn vẹn - Integrity	Đây là nguyên tắc cơ bản của việc giữ thông tin tổ chức chính xác, không có lỗi, và không có sửa đổi trái phép.

Sẵn sàng - Availability	Đây là nguyên tắc cơ bản của việc đảm bảo rằng các hệ thống hoạt động liên tục và người được ủy quyền có thể truy cập các dữ liệu mà họ cần.

Chống chối bỏ

Tính chống chối bỏ là mục tiêu của sự đảm bảo rằng một bên khi gửi một giao dịch hoặc dữ liệu được tạo ra vẫn còn liên kết với dữ liệu đó và không thể phủ nhận việc gửi hoặc tạo ra dữ liệu đó. Bạn sẽ có thể độc lập xác nhận danh tính của một người gửi tin nhắn, và người gửi phải có trách nhiệm đối với các tin nhắn và dữ liệu của nó.

Tính nhận biết

Trong lĩnh vực bảo mật, *tính nhận biết* là một phương pháp để đảm bảo rằng một thực thể yêu cầu truy cập vào tài nguyên bằng cách sử dụng một tập hợp các thông tin quan trọng là chủ sở hữu thực sự của các thông tin. Việc đầu tư và nỗ lực mà đi vào thực hiện một phương pháp nhận dạng khác nhau tùy thuộc vào mức độ bảo mật hoặc sự bảo vệ đó là cần thiết trong một tổ chức.

Xác thực

Xác thực là phương pháp chứng thực một chủ thể cụ thể hoặc các thông tin độc đáo của cá nhân. Chứng thực tập trung vào việc xác định nếu một cá nhân cụ thể có các thông tin bên phải để nhập vào một hệ thống hoặc trang web an toàn.

Ủy quyền

Trong lĩnh vực bảo mật, *ủy quyền* là quá trình xác định các quyền và đặc quyền một chủ thể cụ thể có. Uỷ quyền là tương đương với một kiểm tra danh sách khách mời tại một cuộc tập hợp độc quyền, hoặc kiểm tra vé của bạn khi bạn đi xem phim bảo vệ an ninh.

Kiểm soát truy cập

Kiểm soát truy cập là quá trình xác định và phân quyền cho các nguồn tài nguyên khác nhau, các đối tượng, hoặc dữ liệu.

Kiểm soát truy cập là cách mà ủy quyền được quản lý.

Kế toán và kiểm toán

Trong điều kiện an ninh, *kế toán- Accounting* là quá trình hoạt động theo dõi và hệ thống ghi và truy cập tài nguyên. Kiểm toán là một phần của kế toán trong đó một chuyên gia an ninh kiểm tra các bản ghi của những gì đã được ghi lại.

Đặc quyền tối thiểu - Least Privilege

Nguyên tắc đặc quyền tối thiểu là người sử dụng và phần mềm chỉ nên có mức tối thiểu của việc tiếp cận này là cần thiết cho họ để thực hiện các nhiệm vụ yêu cầu của họ. Đây là cấp độ truy cập tối thiểu bao gồm các trang thiết bị, phần cứng máy tính, phần mềm, và thông tin. Khi một người dùng hoặc hệ thống được trao quyền truy cập, truy cập mà vẫn cần được chỉ ở mức độ cần thiết để thực hiện các nhiệm vụ cần thiết.

Đặt đặc quyền - Privilege Bracketing

Khái niệm *privilege bracketing* được sử dụng khi những đặc quyền được đưa ra chỉ khi cần thiết, sau đó thu hồi ngay khi công việc được hoàn thành hoặc cần thiết đã được thông qua.

Chia sẻ trách nhiệm

Tách nhiệm vụ nói rằng không có một người cần phải có quá nhiều quyền lực và trách nhiệm. Nhiệm vụ và trách nhiệm được chia cho các cá nhân để ngăn chặn xung đột về đạo đức hoặc lạm dụng quyền hạn. Các nhiệm vụ như ủy quyền phê duyệt và thiết kế và phát triển không nên được tổ chức bởi cùng một cá nhân, bởi vì nó sẽ là quá dễ dàng cho người đó để khai thác một tổ chức vào chỉ sử dụng phần mềm cụ thể có chứa lỗ hổng, hoặc tham gia vào các dự án mà có thể mang lại lợi ích cho cá nhân.

Các phương pháp xác thực

Xác thực mạnh là việc đầu tiên của sự phòng chống trong các trận chiến để bảo đảm tài nguyên mạng. Nhưng xác thực không phải là một quá trình duy nhất; có rất nhiều phương pháp và cơ chế khác nhau, một số trong đó thậm chí có thể được kết hợp để tạo thành đề án phức tạp hơn. Là một chuyên gia mạng, làm quen

với các phương pháp xác thực chính trong sử dụng ngày nay có thể giúp bạn thực hiện và hỗ trợ những người thích hợp cho môi trường của bạn.

Xác thực tên tài khoản/ mật khẩu

Sự kết hợp của một tên người dùng và mật khẩu là một trong những đề án xác thực cơ bản nhất và sử dụng rộng rãi. Trong loại này xác thực, thông tin của người dùng được so sánh với các thông tin được lưu trữ trong một cơ sở dữ liệu. Nếu tên người dùng và mật khẩu phù hợp với cơ sở dữ liệu, người dùng được chứng thực. Nếu không, người sử dụng bị từ chối truy cập. Phương pháp này có thể không được rất an toàn vì nó không nhất thiết phải xác định người sử dụng chính xác. Ví dụ, các thông tin của người sử dụng đôi khi được truyền qua mạng trong văn bản không được mã hóa, làm cho tên người dùng và mật khẩu truy cập dễ dàng để một kẻ tấn công.

Tokens

Tokens là các đối tượng vật lý hay ảo, chẳng hạn như thẻ thông minh, thẻ nhân viên, hoặc các gói dữ liệu, đó lưu trữ thông tin xác thực. Tokens có thể lưu trữ số cá nhân nhận dạng (PIN), thông tin về người sử dụng, hoặc mật khẩu. Giá trị thẻ duy nhất có thể được tạo ra bởi các thiết bị đặc biệt hoặc phần mềm để đáp ứng với một thách thức từ một máy chủ chứng thực hoặc bằng cách sử dụng các thuật toán độc lập.

Thẻ thông minh

*Thẻ thông minh l*à một ví dụ phổ biến của chứng thực thẻ

Sinh trắc học

Sinh trắc học là chương trình xác thực dựa trên việc xác định các cá nhân bằng các đặc tính vật lý của họ.

Keystroke Authentication

Keystroke authentication là một loại chứng thực dựa trên các thông tin chi tiết mô tả chính xác khi một phím bàn phím được nhấn và thả như loại người nào đó thông tin vào một máy tính hoặc thiết bị điện tử khác. Mỗi người dùng có xu hướng nhất định, nhịp điệu, và các mẫu khi nói đến cách gõ trên bàn phím, và chúng có thể được ghi lại và đo để so sánh với tổ hợp phím tương lai.

Xác thực đa yếu tố

Xác thực đa yếu tố là bất kỳ cơ chế thẩm định yêu cầu xác nhận của hai hay nhiều yếu tố xác thực. Nó có thể là bất kỳ sự kết hợp của bạn là ai, những gì bạn có, những gì bạn biết, bạn đang ở đâu hay không, và những gì bạn làm.

Các khái niệm về Cryptography

Mật mã - Cryptography

Mật mã là khoa học về che giấu thông tin. Việc thực thi mật mã được cho là ra đời gần như cùng chữ viết. Khoa học mật mã hiện nay có nguồn gốc trong toán học và khoa học máy tính, và phụ thuộc rất nhiều vào công nghệ. Thông tin liên lạc hiện đại và sử dụng mật mã máy tính rộng rãi để bảo vệ thông tin nhạy cảm và thông tin liên lạc từ các truy cập trái phép hoặc tiết lộ tình cờ trong khi thông tin là quá cảnh và trong khi các thông tin đang được lưu trữ.

Sử dụng công nghệ đã được kiểm chứng

Bất kỳ công nghệ mới nào cần phải được kiểm tra chặt chẽ trước khi được áp dụng cho một mạng lưới sản xuất trực tiếp. Riêng với mật mã học, công nghệ và kỹ thuật nên có một lịch sử cũng như các tài liệu điều tra của các chuyên gia ngành công nghiệp.

Mã hóa và giải mã

Mã hóa là một kỹ thuật mật mã có thể chuyển đổi dữ liệu từ bản rõ (plaintext hay cleartext), thành các mã, hay ciphertext. *Giải mã* là các kỹ thuật đồng hành có thể chuyển đổi ciphertext trở lại cleartext.

Phương thức mật mã

Một phương thức mã hóa là một thuật toán được sử dụng để mã hóa hoặc giải mã dữ liệu. Các thuật toán có thể đơn giản là cơ chế thay thế, nhưng trong mật mã điện tử, nó thường là các hàm toán học phức tạp. Càng mạnh thì hàm toán học, càng khó khăn hơn là để phá vỡ mật mã. Plaintext, hay cleartext, là, dữ liệu chưa mã hóa ban đầu. Một khi các thuật toán mã hóa được áp dụng thông qua Enciphering, dữ liệu che khuất được gọi là bản mã. Quá trình ngược lại của dịch ciphertext để cleartext được biết đến như là *giải mã*..

Hashing Encryption

Băm mã hóa là mã hóa một chiều để biến đổi từ cleartext thành ciphertext mà không có ý định để được giải mã. Kết quả của quá trình băm được gọi là một hash, giá trị băm, hoặc tóm lược thông điệp. Các dữ liệu đầu vào có độ dài khác nhau, trong khi chiều dài băm là cố định.

Mã hóa đối xứng

Mã hóa đối xứng là một chương trình mã hóa hai chiều, trong đó mã hóa và giải mã đều được thực hiện bởi cùng một khóa.

.Mã hóa bất đỗi xứng

Mã hóa bất đối xứng sử dụng khóa công khai và cá nhân. Khoá cá nhân được giữ bí mật trong quá trình mã hóa hai chiều. Bởi vì các khóa riêng là không bao giờ chia sẻ, tính bảo mật của nó là đảm bảo.

Khóa công khai được đưa ra cho bất cứ ai. Tùy thuộc vào các ứng dụng của mã hóa, một trong hai bên có thể sử dụng các khóa mã hóa. Các chốt khác trong cặp được sử dụng để giải mã. Các khóa riêng trong một cặp có thể giải mã dữ liệu được mã hóa bằng khóa công khai tương ứng.

Chữ ký số

Chữ ký số là một thông điệp tóm lược đã được mã hóa với khóa riêng của người dùng. Thuật toán mã hóa bất đối xứng có thể được sử dụng với các thuật toán băm để tạo chữ ký kỹ thuật số.

Xác định các mối đe dọa an ninh và lỗ hổng

Social Engineering – tấn công phi kỹ thuật

Khi bạn nghĩ về các cuộc tấn công chống lại các hệ thống thông tin, bạn có thể nghĩ rằng nhất thiết phải bảo vệ các thành phần công nghệ của các hệ thống. Nhưng bản thân con người - những người dùng hệ thống – cũng là một phần của một hệ thống thông tin như các thành phần công nghệ; họ có lỗ hổng riêng của họ, và họ có thể là phần đầu tiên của hệ thống để chống chọi lại với một số loại tấn công.

Tấn công Social engineering

Một cuộc tấn công social engineering là một loại tấn công mà sử dụng sự lừa dối và lừa gạt để thuyết phục người dùng không nghi ngờ cung cấp dữ liệu nhạy cảm hoặc vi phạm nguyên tắc bảo mật. Kỹ thuật xã hội thường là một tiền thân của một loại tấn công. Bởi vì các cuộc tấn công phụ thuộc vào yếu tố con người chứ không phải là về công nghệ, các triệu chứng của họ có thể mơ hồ và khó xác định. Tấn công kỹ thuật xã hội có thể đến trong một loạt các phương pháp: trực tiếp, qua email, hoặc qua điện thoại.

VoIP

VoIP là một công nghệ cho phép bạn để cung cấp thông tin điện thoại qua mạng IP. Các thông tin bằng giọng nói sẽ được gửi qua mạng IP ở dạng kỹ thuật số trong các gói dữ liệu, so với việc thực hiện trên Public Switched Telephone Network (PSTN) trong đó bao gồm các giao thức đảm bảo kết nối.

Tin tặc và những kẻ tấn công

Tin tặc và những kẻ tấn công là những thuật ngữ liên quan cho những cá nhân có kỹ năng để đạt được quyền truy cập vào hệ thống máy tính thông qua các phương tiện không được phép hoặc không được chấp thuận. Nguyên, hacker là một thuật ngữ trung tính cho một người dùng xuất sắc trong lập trình máy tính và quản trị hệ thống máy tính. Hack vào một hệ thống đã được một dấu hiệu của kỹ năng kỹ thuật và sự sáng tạo mà dần dần trở thành liên kết với sự xâm nhập hệ thống bất hợp pháp hoặc độc hại. Kẻ tấn công là một thuật ngữ luôn là một hệ thống kẻ xâm nhập nguy hiểm.

Malware

Một trong những mối đe dọa phổ biến nhất đối với máy tính ngày nay là mã độc. Là một chuyên gia bảo mật, hoặc thậm chí là một người sử dụng máy tính thường xuyên, bạn có thể sẽ có nhiều kinh nghiệm trong việc đối phó với các phần mềm không mong muốn lây nhiễm hệ thống của bạn. Malware xảo quyệt và khó khăn để loại bỏ, do đó, nó có thể gây ra một số lượng đáng kể thiệt hại theo nhiều cách khác nhau.

Tấn công mã độc

Một cuộc tấn công mã độc là một loại tấn công phần mềm mà một kẻ tấn công chèn một số loại không mong muốn hoặc không được phép phần mềm, hoặc phần mềm độc hại, vào một hệ thống mục tiêu. Trong quá khứ, nhiều cuộc tấn công mã độc hại được dự định để làm gián đoạn hoặc vô hiệu hóa một hệ thống điều hành hoặc một ứng dụng, hoặc buộc các hệ thống mục tiêu để phá vỡ hoặc vô hiệu hóa các hệ thống khác. Nhiều cuộc tấn công mã độc gần đây cố gắng để ẩn đi trên hệ thống mục tiêu, nguồn lực có sẵn để lợi thế của kẻ tấn công.

Viruses

Vi rút là một đoạn mã đó lây lan từ máy này sang máy khác bằng cách gắn nó vào các file khác thông qua một quá trình tự sao chép. Các mã trong một virus thực thi khi các tập tin được đính kèm theo được mở ra. Thông thường, loại virus này đã có ý định cho phép tiếp tục tấn công, gửi dữ liệu trở lại cho kẻ tấn công, hoặc thậm chí bị hỏng hoặc phá hủy dữ liệu. Bởi vì bản chất tự sao chép của nó, virus rất khó để gỡ bỏ hoàn toàn từ một hệ thống và chiếm tỷ đô la thiệt hại mỗi năm.

Worms

Trong máy tính, một con sâu là malware mà, như virus, nó có thể sao chép chính nó trên hệ thống bị nhiễm. Tuy nhiên, không giống như một virus, nó không tự gắn vào các chương trình hoặc các file khác. Trong khi virus có xu hướng can thiệp vào các chức năng của một máy tính cụ thể, sâu thường được dùng để làm gián đoạn khả năng của mạng. Worms thường biến máy tính thành zombie từ xa mà kẻ tấn công có thể sử dụng để khởi động các cuộc tấn công khác từ.

Adware - Phần mềm quảng cáo

Adware là phần mềm tự động hiển thị quảng cáo không mong muốn hoặc tải khi nó được sử dụng. Phần mềm quảng cáo thường xuất hiện trên máy tính của người sử dụng như một trình duyệt pop-up. Trong khi không phải tất cả các phần mềm quảng cáo là công khai độc hại, nhiều chương trình phần mềm quảng cáo có liên quan đến phần mềm gián điệp và các loại phần mềm độc hại. Ngoài ra, nó có thể làm giảm năng suất người dùng bằng cách làm chậm hệ thống và đơn giản chỉ là một ít phiền toái.

Spyware - Phần mềm gián điệp

Phần mềm gián điệp là lén lút cài đặt phần mềm độc hại mà có thể dùng để theo dõi và báo cáo việc sử dụng một hệ thống mục tiêu, hoặc thu thập dữ liệu khác tác giả mong muốn có được. Số liệu thu thập có thể bao gồm lịch sử duyệt web, thông tin cá nhân, ngân hàng và các thông tin tài chính khác, và tên người dùng và mật khẩu. Mặc dù nó có thể lây nhiễm sang một máy tính thông qua các chiến thuật kỹ thuật xã hội, một số phần mềm gián điệp được kèm với các phần mềm khác hợp pháp

.Trojan Horses

A *Trojan horse*, thường gọi đơn giản là một Trojan, được giấu phần mềm độc hại là nguyên nhân gây thiệt hại cho một hệ thống hoặc cho một kẻ tấn công một nền tảng cho việc giám sát và / hoặc kiểm soát một hệ thống. Không giống như virus, Trojan không tự nhân bản, cũng không đính kèm các tập tin khác. Thay vào đó, họ thường là xảo quyệt hơn và không bị phát hiện dễ dàng hơn. Trojan thường được nhân giống bằng kỹ thuật xã hội, chẳng hạn như khi người dùng download một file đính kèm email tuyên bố rằng là lành tính, nhưng thực sự là ác tính.

Rootkits

Rootkit là mã được dùng để kiểm soát toàn bộ hoặc một phần của một hệ thống ở mức thấp nhất. Rootkits thường cố gắng che giấu bản thân từ việc giám sát hoặc phát hiện và sửa đổi các tập tin hệ thống cấp thấp khi kết hợp với nhau thành một hệ thống. Rootkit có thể được sử dụng cho các mục đích không độc hại như ảo hóa; Tuy nhiên, hầu hết các bệnh nhiễm trùng rootkit cài đặt backdoor, spyware, hoặc mã độc hại khác một khi họ có quyền kiểm soát của hệ thống đích.

Logic Bombs

Một quả bom logic là một đoạn mã mà ngồi im lìm trên một máy tính mục tiêu cho đến khi nó được kích hoạt bởi một sự kiện cụ thể, chẳng hạn như một ngày cụ thể. Một khi các mã được kích hoạt, những quả bom nổ luận, và thực hiện bất cứ hành động đó đã được lập trình để làm. Thông thường, điều này bao gồm tẩy xoá và làm hư dữ liệu trên hệ thống đích.

Botnets

Một *botnet* là một tập hợp các máy tính đã bị nhiễm bởi một chương trình kiểm soát gọi là bot cho phép kẻ tấn công để khai thác chung các máy tính để gắn kết các cuộc tấn công. Thông thường, mũ đen sử dụng botnet để phối hợp tấn công từ chối dịch vụ, gửi thư rác, và của tôi để biết thông tin cá nhân hoặc mật khẩu. Người sử dụng các máy tính bị nhiễm (gọi là zombie hay drone) thường không biết rằng máy tính của họ đang được sử dụng cho các mục đích bất chính.

Ransomware

Ransomware là một malware ngày càng phổ biến, trong đó kẻ tấn công lây nhiễm máy tính của nạn nhân với mã đó hạn chế truy cập của nạn nhân để máy tính của họ hoặc các dữ liệu trên đó. Sau đó, những kẻ tấn công đòi một khoản tiền chuộc được trả tiền, thường là thông qua một dịch vụ thanh toán trực tuyến như PayPal hoặc Green Dot MoneyPak, đe dọa của việc giữ các hạn chế hoặc phá hủy các thông tin mà họ đã khóa.

Malware Đa hình

Để làm cho họ khó khăn hơn để phát hiện, những kẻ tấn công đã bắt đầu mã hóa virus để chúng sẽ lây nhiễm các tập tin với một bản sao mã hóa của mình. Các khóa mật mã và giải mã một mô-đun sẽ được bao gồm với các virus và được lưu trữ trong bản rõ. Các máy quét chống virus sau đó sẽ cần để phát hiện virus gián tiếp thông qua các module giải mã. Phần mềm độc hại đa hình sử dụng mã hóa này vi-rút tương tự, chỉ module giải mã được thay đổi mỗi khi virus lây nhiễm vào một tập tin. Điều này làm cho nó rất khó khăn cho các phần mềm chống virus để phát hiện một bệnh nhiễm trùng được thay đổi liên tục.

Armored Viruses

Chất lượng xác định của virus bọc thép là họ cố gắng để lừa hoặc che chắn mình từ phần mềm chống virus và các chuyên gia an ninh. Để đánh lừa các phần mềm chống virus, một con virus bọc thép có khả năng làm mờ đúng vị trí của nó trong một hệ thống và dẫn các phần mềm để tin rằng nó nằm ở nơi khác. Điều này ngăn cản các phần mềm chống virus từ phát hiện chính xác và loại bỏ các nhiễm trùng. Tương tự như vậy, virus bọc thép thường chứa obfuscated mã để làm cho

nó khó khăn hơn cho các nhà nghiên cứu bảo mật để đánh giá và thiết kế đối chiếu chúng đúng cách.

Sự cố trên thế giới thực

Sự thật lạ hơn viễn tưởng. Từ mối tình bất chính văn phòng tới trộm cắp thiết bị, từ biển thủ tài sản trí tuệ đang bị truy cứu email spam, sự đa dạng là tuyệt vời. Một trong những điều các sự cố đã có điểm chung là sự tham gia của các máy tính.

Máy tính và mạng có liên quan đến hầu như tất cả các hoạt động ngày hôm nay. Các tính chất phổ biến của máy tính và mạng có nghĩa là nó đang ngày càng kết nối với các sự cố và tội phạm.

Các yếu tố ảnh hưởng đến phản ứng

Nhiều yếu tố ảnh hưởng đến cách một sự cố được xử lý. Có pháp lý, chính trị, kinh doanh, và các yếu tố kỹ thuật mà sẽ định hình mọi điều tra.

Tội phạm Quốc tế

Ở đầu kia của quang phổ tội phạm máy tính là những trường hợp liên quan đến kẻ tấn công độc hại và trộm cắp kinh tế.

Hacks truyền thống

Mặc dù có rất nhiều sự cố, một trường hợp gần đây là một ví dụ tốt về một loại vẫn còn phổ biến của vụ việc mà tổ chức phải giải quyết. Ngày 25 Tháng 1 2003, một quản trị viên an ninh tại một ngân hàng khu vực nghĩ rằng ông đã tăng cường các quy luật đặt trên một router Cisco IP bằng cách áp dụng câu lệnh *IP permit any any* ở dòng quy tắc đầu tiên. Trên router Cisco, các quy tắc được áp dụng theo thứ tự. Như quy tắc đầu tiên trong danh sách, dòng lệnh này có tác dụng loại bỏ bất kỳ hạn chế truy cập các router đã được cung cấp. Router cụ thể này đã được sử dụng để bảo vệ một "khu vực phi quân sự" trực tiếp với Internet (DMZ).

Giới thiệu về ứng phó sự cố

Một sự cố an ninh máy tính là gì?

Một sự cố an ninh máy tính là bất kỳ hành động trái pháp luật, trái phép, hoặc không thể chấp nhận có liên quan đến một hệ thống máy tính hoặc một mạng máy tính. Một hành động như vậy có thể bao gồm bất kỳ các sự kiện sau đây:

- Trộm cắp bí mật thương mạiemail spam or harassment
- Xâm nhập trái phép hoặc bất hợp pháp vào hệ thống máy tính
- Biển thủ
- Kiểm soát bóng, phổ biến các nội dung khiêu dâm trẻ em
- (dos) tấn công Denial-of-dịch vụ
- Nhiễu có hại của quan hệ kinh doanh
- Tống tiền
- Bất kỳ hành động trái pháp luật khi các bằng chứng về những hành động đó có thể được lưu trữ trên phương tiện truyền thông máy tính như là gian lận, các mối đe dọa, và tội phạm truyền thống.

Các mục tiêu của ứng phó sự cố là gì?

Trong phương pháp ứng phó sự cố của chúng tôi, chúng tôi nhấn mạnh mục tiêu của các chuyên gia bảo mật của công ty với mối quan tâm kinh doanh hợp pháp, nhưng chúng tôi cũng đi vào xem xét các mối quan tâm của các quan chức thực thi pháp luật. Vì vậy, chúng tôi đã phát triển một phương pháp nhằm thúc đẩy một phối hợp, phản ứng gắn kết và đạt được những điều sau đây:

- Ngăn chặn một phản ứng noncohesive rời rạc (mà có thể là thảm họa)
- Xác nhận hoặc xua đi xem một sự cố xảy ra
- Khuyến khích tích tụ các thông tin chính xác
- Thiết lập các điều khiển để thu hồi thích hợp và xử lý tang
- Bảo vệ quyền riêng tư được thành lập theo pháp luật và chính sách
- Giảm thiểu sự gián đoạn cho hoạt động kinh doanh và mạng
- Cho phép để hành động hình sự hoặc dân sự đối với thủ phạm
- Cung cấp các báo cáo chính xác và khuyến nghị hữu ích

- Cung cấp nhanh chóng phát hiện và ngăn chặn
- Giảm thiểu tiếp xúc và sự thỏa hiệp của dữ liệu độc quyền
- Bảo vệ danh tiếng và tài sản của tổ chức
- Quản lý cấp cao của giáo dục
- Khuyến khích phát hiện nhanh và / hoặc phòng ngừa các sự cố như vậy trong tương lai (thông qua bài học kinh nghiệm, những thay đổi chính sách, vv)

Ai tham gia vào quá trình ứng phó sự cố?

Xử lý sự cố là một kỷ luật nhiều mặt. Nó đòi hỏi vô số các khả năng mà thường đòi hỏi nguồn lực từ các đơn vị hoạt động khác nhau của một tổ chức. Nhân viên nhân sự, tư vấn pháp lý, các chuyên gia kỹ thuật, các chuyên gia an ninh, nhân viên an ninh của công ty, các nhà quản lý kinh doanh, người sử dụng cuối cùng, công nhân viên hỗ trợ, và các nhân viên khác mayfind mình tham gia ứng phó với sự cố acomputersecurity.

Hầu hết các tổ chức thành lập một nhóm các cá nhân, thường được gọi là một Đội ứng cứu sự cố bảo mật máy tính (CSIRT), để đối phó với bất kỳ sự cố an ninh máy tính. Các CSIRT là một đội ngũ nhiều thành phần phù hợp pháp lý, kỹ thuật, và các lĩnh vực cần thiết để giải quyết sự cố.

Phương pháp ứng phó sự cố

Sự cố an ninh máy tính thường là các vấn đề rất phức tạp, đa diện.Có bảy thành phần chính của phản ứng sự cố:

- **Chuẩn bị trước sự cố** Hãy hành động để chuẩn bị các tổ chức và CSIRT trước khi xảy ra sự cố.
- **Phát hiện sự cố** Xác định một sự cố an ninh máy tính tiềm năng.
- **Phản ứng ban đầu** Thực hiện một cuộc điều tra ban đầu, ghi lại các chi tiết cơ bản xung quanh vụ việc, lắp ráp đội ứng phó sự cố, và thông báo cho cá nhân, những người cần phải biết về vụ việc.
- **Xây dựng chiến lược phản ứng** Dựa trên kết quả của tất cả các sự kiện được biết, xác định phản ứng tốt nhất và được sự chấp thuận quản lý. Xác định dân sự, hình sự, hành chính, hoặc các hành động thích hợp để thực hiện, dựa trên các kết luận rút ra từ cuộc điều tra.

- **Điều tra vụ việc** Thực hiện một bộ sưu tập toàn diện của dữ liệu. Xem lại các dữ liệu thu thập được để xác định những gì đã xảy ra, khi nó đã xảy ra, những người đã làm nó, và làm thế nào nó có thể được ngăn chặn trong tương lai.
- **Báo cáo chính xác** báo cáo thông tin về cuộc điều tra một cách hữu ích cho các nhà sản xuất quyết định.
- **Giải pháp** Nghị quyết sử dụng và những thay đổi về thủ tục, hồ sơ bài học học được, và phát triển các bản sửa lỗi lâu dài cho bất kỳ vấn đề xác định.

Phát hiện sự cố

Nếu một tổ chức không thể phát hiện sự cố một cách hiệu quả, nó không thể thành công trong việc ứng phó với các sự cố. Vì vậy, việc phát hiện các sự cố là một trong những khía cạnh quan trọng nhất của ứng phó sự cố. Nó cũng là một trong những giai đoạn phân cấp nhất, trong đó những người có chuyên môn ứng phó sự cố có sự kiểm soát nhất.

Phản ứng ban đầu

Một trong những bước đầu tiên của bất kỳ điều tra là để có được đầy đủ thông tin để xác định một phản ứng thích hợp. Giai đoạn phản ứng ban đầu liên quan đến việc tập hợp các CSIRT, thu thập dữ liệu dựa trên mạng và dữ liệu khác, việc xác định các loại vụ việc đó đã xảy ra, và đánh giá tác động của vụ việc. Ý tưởng là để thu thập đủ thông tin để bắt đầu giai đoạn tiếp theo, đó là phát triển một chiến lược phản ứng. Mục đích khác của giai đoạn phản ứng ban đầu là tài liệu hóa các bước phải được thực hiện. Cách tiếp cận này ngăn chặn các phản ứng "knee-jerk" và hoảng loạn khi một sự cố được phát hiện, cho phép tổ chức của bạn để thực hiện một phương pháp tiếp cận ở giữa một tình huống căng thẳng.

Xây dựng một chiến lược ứng phó

Mục tiêu của giai đoạn xây dựng chiến lược phản ứng là để xác định các chiến lược đối phó phù hợp nhất, cho các trường hợp xảy ra sự việc. Chiến lược nên đi vào xem xét, kỹ thuật, pháp lý, và các yếu tố kinh tế chính trị xung quanh vụ việc. Các giải pháp cuối cùng phụ thuộc vào các mục tiêu của nhóm hay cá nhân với trách nhiệm lựa chọn chiến lược.

Xét tổng thể của hoàn cảnh

Xem xét các xử lý thích hợp

Điều tra sự cố

Giai đoạn điều tra liên quan đến việc xác định ai, cái gì, khi nào, ở đâu, như thế nào, và tại sao xung quanh một sự cố. Bạn sẽ tiến hành việc điều tra, xem xét các bằng chứng dựa trên máy chủ, bằng chứng dựa trên mạng, và bằng chứng thu thập được thông qua truyền thống, bước điều tra không kỹ thuật.

Thu thập dữ liệu

Phân tích pháp y

Báo cáo

Báo cáo có thể là giai đoạn khó khăn nhất của quá trình ứng phó sự cố. Thách thức là tạo ra các báo cáo mô tả chính xác các chi tiết của một sự cố, nó là dễ hiểu đối với người ra quyết định, có thể chịu được sự dung túng của giám sát pháp lý, và được sản xuất một cách kịp thời.

- **Tài liệu ngay lập tức**
- **Viết ngắn gọn và rõ ràng**
- **Sử dụng một định dạng chuẩn**

Giải pháp

Mục tiêu của giai đoạn giải pháp là để thực hiện dựa trên máy chủ, dựa trên mạng, và biện pháp đối phó thủ tục để ngăn chặn một sự cố gây thiệt hại hơn nữa và trở về tổ chức của bạn về tình trạng hoạt động lành mạnh an toàn. Nói cách khác, trong giai đoạn này, bạn có các vấn đề, giải quyết vấn đề, và thực hiện các bước để ngăn chặn vấn đề này xảy ra một lần nữa.

Chương 2: Đánh giá rủi ro

Giới thiệu

Đánh giá rủi ro an ninh

Đây là hoạt động để đo sức mạnh của các chương trình bảo mật tổng thể và cung cấp các thông tin cần thiết để thực hiện kế hoạch cải tiến dựa trên rủi ro an ninh thông tin. Các đánh giá rủi ro an ninh là công cụ của quản lý cấp cao cung cấp cho họ một đo lường hiệu quả của kiểm soát an ninh của họ và chỉ ra tài sản của họ được bảo vệ như thế nào.

Vai trò của đánh giá rủi ro an ninh

Một đánh giá rủi ro bảo mật là yếu tố quan trọng trong quá trình quản lý rủi ro an ninh tổng thể. Quản lý rủi ro bảo mật liên quan đến quá trình đảm bảo rằng các rủi ro của một tổ chức là trong giới hạn chấp nhận được theo quy định của quản lý cấp cao. Có bốn giai đoạn của quá trình quản lý rủi ro an ninh: đánh giá rủi ro an ninh; kiểm tra và xem xét lại; giảm thiểu rủi ro an ninh; và an ninh hoạt động

Định nghĩa của việc đánh giá rủi ro an ninh

Các đánh giá rủi ro an ninh mất trên nhiều tên và có thể khác nhau rất nhiều về phương pháp, sự chặt chẽ, và phạm vi, nhưng mục tiêu cốt lõi vẫn là giống nhau: đánh giá rủi ro đối với tài sản thông tin của tổ chức. Thông tin này được sử dụng để xác định cách tốt nhất để giảm thiểu những rủi ro và bảo tồn có hiệu quả nhiệm vụ của tổ chức.

Sự cần thiết của một đánh giá rủi ro an ninh

Ngoài việc yêu cầu, đánh giá rủi ro bảo mật là một yếu tố thiết yếu của bất kỳ công ty tìm cách bảo vệ tài sản thông tin của nó. Một đánh giá rủi ro an ninh có những lợi ích sau đây để một tổ chức.

- Kiểm tra và Cân bằng
- Đánh giá định kỳ
- Chi dựa trên rủi ro

- Yêu cầu

Khái niệm cơ bản đánh giá rủi ro an ninh thông tin

Đối với mục đích của cuốn sách này, quá trình đánh giá rủi ro an ninh thông tin được định nghĩa là "một phân tích khách quan về hiệu quả của các kiểm soát an ninh hiện tại để bảo vệ tài sản của một tổ chức và một quyết tâm của xác suất thiệt hại cho tài sản đó". Có nhiều phương pháp có sẵn và đang được sử dụng. Tùy thuộc vào việc đánh giá nguy cơ an ninh cụ thể làm việc, đánh giá rủi ro an ninh có thể có bất kỳ số lượng các bước hoặc các giai đoạn, nhưng quá trình tổng thể phần lớn là tương tự như trong tất cả các phương pháp này.

Giai đoạn 1: Định nghĩa dự án

Như với nhiều dự án, sự thành công của dự án đánh giá rủi ro an ninh không chỉ dựa vào kỹ năng và kinh nghiệm của đội ngũ giao cho việc đánh giá nguy cơ an ninh mà còn về hiệu quả của việc quản lý dự án. Một thành phần quan trọng của quản lý dự án đã được chuyển đến một thỏa thuận đối với các phạm vi và nội dung của phân phôi. Trong giai đoạn định nghĩa dự án, dự án là xác định phạm vi và tài liệu đúng.

Giai đoạn 2: Chuẩn bị dự án

Căn cứ vào phạm vi của dự án đánh giá rủi ro an ninh xác định trong giai đoạn 1, lãnh đạo đội bóng cần phải đảm bảo rằng các chế đầy đủ được thực hiện trước khi bước vào giai đoạn thu thập dữ liệu. Chuẩn bị bao gồm việc chuẩn bị đội ngũ và chuẩn bị dự án.

Giai đoạn 3: Thu thập dữ liệu

Giai đoạn thu thập dữ liệu thường được thực hiện trực tiếp (on site) và kết quả thu thập thông tin liên quan đến hiệu quả của các điều khiển bảo mật quản trị, vật lý và kỹ thuật hiện hành. Nhóm nghiên cứu đánh giá rủi ro an ninh sẽ xem xét lại các điều khiển hành chính thông qua việc thu thập, đánh giá, phân tích chính sách có sẵn, thủ tục, và quan sát và phỏng vấn với các nhân viên. Việc kiểm soát an ninh vật lý sẽ được đánh giá thông qua các kỹ thuật như quan sát, thử nghiệm

và phân tích. Các điều khiển an ninh kỹ thuật sẽ được xem xét thông qua phân tích kỹ thuật, thử nghiệm, và xem xét lại các bản ghi.

Giai đoạn 4: Phân tích rủi ro

Giai đoạn phân tích rủi ro liên quan đến việc xem xét lại các dữ liệu thu thập và phân tích các nguy cơ đối với tổ chức. Trong giai đoạn này, nhóm đánh giá rủi ro an ninh phải xác định giá trị tài sản, hệ thống quan trọng, khả năng bị đe dọa, và sự tồn tại của lỗ hổng bảo mật dựa trên các dữ liệu thu thập được. Hơn nữa, các đội phải tính toán rủi ro cho các tổ chức cho từng cặp mối đe dọa / dễ bị tổn thương. Việc tính toán và trình bày các rủi ro có thể khác nhau rất nhiều, tùy thuộc vào phương pháp đánh giá rủi ro an ninh đang được sử dụng.

Một số yếu tố của giai đoạn phân tích rủi ro được coi là khái niệm quan trọng trong đánh giá rủi ro an ninh. Chúng bao gồm các tài sản, các mối đe dọa, lỗ hổng, và nguy cơ bảo mật.

Tài sản

Yếu tố đầu tiên được xem xét và thảo luận trong một đánh giá rủi ro an ninh thông tin là tài sản của tổ chức. Tài sản là những mặt hàng có giá trị xem xét bởi tổ chức, là những thông tin và tài nguyên có giá trị cho tổ chức. Các ví dụ bao gồm các tòa nhà, thiết bị, nhân lực, uy tín tổ chức, tài liệu kinh doanh, và nhiều mặt hàng hữu hình và vô hình khác.

Các mối đe dọa và tác nhân

Các yếu tố tiếp theo được xem xét và thảo luận trong một đánh giá rủi ro an ninh thông tin là những mối đe dọa và các tác nhân đe dọa. Một mối đe dọa là một sự kiện có tác động không mong muốn. Tác nhân đe dọa là thực thể mà có thể làm một mối đe dọa xảy ra. Các mối đe dọa và các tác nhân đe dọa được gắn bó chặt chẽ trong đó nó là tác nhân đe dọa gây ra một mối đe dọa xảy ra.

Giai đoạn 5: Giảm thiểu Rủi ro

Dựa trên những rủi ro được xác định trong giai đoạn phân tích rủi ro, các đội phải phát triển các khuyến nghị cho các biện pháp bảo vệ để giảm các rủi ro được xác định đến một mức độ chấp nhận được. Quá trình lựa chọn an toàn liên quan đến biện pháp bảo vệ lập bản đồ cho các cặp mối đe dọa / lỗ hổng, xác định

việc giảm nguy cơ, xác định chi phí của tự vệ, và nhóm các biện pháp bảo vệ vào bộ giải pháp.

Một số yếu tố của giai đoạn giảm thiểu rủi ro được coi là khái niệm quan trọng trong đánh giá rủi ro an ninh. Chúng bao gồm các biện pháp bảo vệ và nguy cơ tồn.

Rủi ro an ninh còn lại

Rủi ro bảo mật còn lại là các rủi ro bảo mật còn lại sau khi thực hiện các biện pháp bảo vệ được đề nghị. Mục tiêu của quản lý rủi ro an ninh là để đo lường chính xác các rủi ro bảo mật còn lại và giữ nó ở mức bằng hoặc thấp hơn mức độ chịu đựng rủi ro an ninh.

Giai đoạn 6: Báo cáo rủi ro và Giải pháp

Giai đoạn cuối cùng của việc đánh giá rủi ro an ninh là các báo cáo rủi ro và giai đoạn thực hiện giải pháp. Trong giai đoạn này, nhóm nghiên cứu đánh giá rủi ro an ninh phát triển một bản báo cáo và trình bày trước các nhà tài trợ dự án xác định rõ các rủi ro được tìm thấy và các biện pháp bảo vệ được đề nghị. Báo cáo đánh giá rủi ro cuối cùng nên cung cấp thông tin rõ ràng cho việc điều hành, quản lý, và nhân viên kỹ thuật. Sau đó việc quản lý điều hành của các tổ chức đánh giá phải xác định độ phân giải của các rủi ro được xác định. Các yếu tố độ phân giải rủi ro trong giai đoạn này được coi là một khái niệm quan trọng trong đánh giá rủi ro an ninh.

Giải quyết rủi ro

Định nghĩa	Giải quyết rủi ro là quyết định của quản lý cấp cao như thế nào để giải quyết các rủi ro đã bực bội với họ	
Khái niệm chính	Giảm thiểu rủi ro	Việc giảm rủi ro cho tổ chức đến một mức độ chấp nhận được thông qua việc áp dụng các điều khiển bảo mật bổ sung hoặc cải thiện các điều khiển hiện tại
	Chấp nhận rủi ro	Các quyết định có chủ ý của quản lý cấp cao để chấp nhận một rủi ro được xác định dựa trên các mục tiêu kinh doanh của tổ chức

	Chuyển hướng rủi ro	Việc chuyển giao hợp đồng rủi ro đối với một tổ chức khác thông qua gia công phần mềm, bảo hiểm

Định nghĩa dự án

Một đánh giá rủi ro an ninh có thể có nghĩa là nhiều việc với nhiều người. Trong bối cảnh của cuốn sách này, một đánh giá rủi ro an ninh được định nghĩa là " một phân tích về hiệu quả của việc kiểm soát hành chính, vật lý và kỹ thuật hiện cùng nhau bảo vệ tài sản của tổ chức. " Quy định khác nhau, hướng dẫn, và các nguồn thông tin khác đôi khi gọi các đánh giá rủi ro bảo mật bằng một cái tên khác. Điều khoản sử dụng bao gồm kiểm toán an ninh, đánh giá rủi ro, kiểm tra an ninh, và như vậy. Những lần khác, một " đánh giá rủi ro an ninh, " được sử dụng để có nghĩa là một cái gì đó khác với những gì chúng tôi mô tả trong cuốn sách này.

Đảm bảo thành công của dự án

Thực hiện đánh giá rủi ro an ninh là một dự án và, như vậy, bất cứ ai tìm cách trở thành một thành viên hiệu quả của một nhóm đánh giá nguy cơ an ninh cần phải hiểu làm thế nào một dự án như vậy được chạy thành công. Hơn nữa, các nhà lãnh đạo của các nhóm đánh giá nguy cơ an ninh cần phải có khả năng lập kế hoạch, theo dõi, và đảm bảo sự thành công của dự án đánh giá rủi ro.

Định nghĩa thành công

Thành công không thể đạt được cho đến khi chúng ta xác định ý nghĩa của thành công. Đối với một dự án đánh giá rủi ro, thành công được định nghĩa là đạt được sự hài lòng của khách hàng, công việc kỹ thuật chất lượng, và hoàn thành dự án trong ngân sách.

- Sự hài lòng của khách hàng
- Chất lượng công việc
- Hoàn thành trong vòng ngân sách

Xác định mục tiêu

Một đánh giá rủi ro an ninh có thể cung cấp nhiều lợi ích có thể có: một cơ sở cho việc chi tiêu dựa trên rủi ro, đánh giá định kỳ các chương trình bảo mật, và một phần của một hệ thống kiểm tra và cân đối với nhiệm vụ nhạy cảm. Sự hiểu biết và tài liệu về mục tiêu của đánh giá rủi ro an ninh cụ thể giúp tập trung dự án vào việc đáp ứng các nhu cầu của tổ chức. Cốt lõi của một đánh giá rủi ro an ninh vẫn là một phân tích về hiệu quả của các kiểm soát an ninh hiện nay để bảo vệ tài sản của tổ chức. Đây là mục tiêu của việc đánh giá rủi ro an ninh.

Mục tiêu đánh giá rủi ro an ninh : phân tích chính xác về hiệu quả của kiểm soát an ninh hiện nay để bảo vệ tài sản của tổ chức.

Giới hạn phạm vi

Phạm vi của việc đánh giá rủi ro an ninh là ranh giới của các kiểm soát an ninh và tài sản trong tổng quan. Định nghĩa của những gì là "đầu vào" và "đầu ra" của các phạm vi của việc đánh giá có thể được khá dễ dàng trong một số tổ chức nhưng khó khăn hơn ở những người khác. Trong cả hai trường hợp, các nhà tài trợ dự án và nhóm đánh giá rủi ro an ninh một cách cẩn thận và rõ ràng nên xác định phạm vi đánh giá về các kiểm soát an ninh để được xem xét lại, các tài sản được bảo vệ, và ranh giới hệ thống của các mục tiêu đánh giá rủi ro an ninh.

Underscoping

Underscoping của một đánh giá rủi ro an ninh là một thực tế nguy hiểm có thể xảy ra quá thường xuyên. Nó xảy ra khi nhóm nghiên cứu đánh giá rủi ro an ninh không giải quyết tất cả các vấn đề an ninh của các nhà tài trợ. Thuật ngữ " underscoping " là từ quan điểm của các nhóm đánh giá nguy cơ an ninh và không tài trợ dự án. Nói cách khác, nhóm nghiên cứu đánh giá rủi ro an ninh không được giải quyết nhu cầu của các nhà tài trợ dự án bởi vì một số tài sản của tổ chức và các mối đe dọa có liên quan không được đánh giá trong đánh giá rủi ro an ninh.

Overscoping

Overscoping của một đánh giá rủi ro an ninh là nguy hiểm là tốt. Overscoping xảy ra khi nhóm nghiên cứu đánh giá rủi ro an ninh đánh giá các mối đe dọa, lỗ hổng, hoặc rủi ro nằm ngoài giới hạn của đánh giá rủi ro an ninh. Thuật ngữ " overscoping " là từ quan điểm của các nhóm đánh giá nguy cơ an ninh và không tài trợ dự án. Nói cách khác, nhóm nghiên cứu đánh giá rủi ro an ninh được tổ chức đánh giá tài sản và các mối đe dọa mà là vượt quá nhu cầu của các nhà tài trợ đánh giá rủi ro an ninh. Nếu một nhà tài trợ dự án không ghi rõ các giới hạn của đánh giá rủi ro an ninh, nhóm nghiên cứu có thể thực hiện các hoạt động mà kết thúc lãng phí thời gian và tiền bạc. Một nguy cơ overscoping là đội bóng đánh giá rủi ro an ninh có thể vượt qua quyền lực của mình để kiểm tra các yếu tố của một hệ thống mà không được bảo hiểm theo đánh giá rủi ro an ninh. Những hành động ngoài quyền đó, tự nó, là một sự vi phạm nghiêm trọng về an ninh.

Điều khiển bảo mật

Một tổ chức có thể đã thực hiện một loạt các kiểm soát an ninh để bảo vệ tài sản của mình. Những điều khiển an ninh có thể dao động từ chính sách và thủ tục để chiếu sáng và hàng rào để tường lửa và các giải pháp chống virus. Thay vì danh sách các điều khiển sau khi khác, nó rất hữu ích để nhóm các điều khiển vào các chuyên mục của hành chính, vật lý và kỹ thuật. Những nhóm cung cấp một phương pháp phổ biến để xác định hoặc giới hạn phạm vi của việc đánh giá rủi ro an ninh.

Tài sản

Tài sản được định nghĩa là các nguồn lực do mà tổ chức này có được giá trị. Đây có thể bao gồm phần cứng, phần mềm, hệ thống, dịch vụ, tài liệu, thiết bị vốn, tài sản cá nhân, con người, thiện chí, bí mật thương mại, và nhiều yếu tố khác của quá trình kinh doanh. Mặc dù rõ ràng rằng nhiều yếu tố tạo ra giá trị cho một tổ chức, nó không phải là luôn luôn dễ dàng để xác định tài sản của mình. Một nỗ lực để đơn giản hóa quá trình liệt kê bao gồm thảo luận về tài sản cả hữu hình và vô hình.

Sự hợp lý trong giới hạn phạm vi

Như đã thảo luận trước đó, không phải tất cả các điều khiển bảo mật hoặc tài sản có thể trong phạm vi của việc đánh giá rủi ro an ninh. Mặc dù, là các chuyên gia bảo mật, chúng tôi thường thấy quy trình đánh giá rủi ro an ninh không bị cản

trở bởi một phạm vi nhỏ hơn được bảo hành, có rất nhiều lý do chính đáng cho việc hạn chế phạm vi của một đánh giá rủi ro an ninh.

Xác định ranh giới hệ thống

Rõ ràng rằng việc không đúng phạm vi đánh giá rủi ro an ninh có thể có hậu quả tai hại. Một yếu tố quan trọng của xác định phạm vi hiệu quả đánh giá rủi ro an ninh là để xác định hệ thống (hoặc các hệ thống) được đánh giá. Một hệ thống thông tin là bất kỳ quá trình, hoặc nhóm các quy trình liên quan, dưới quyền chỉ huy, quản lý kiểm soát duy nhất nằm trong cùng một môi trường hoạt động chung. Các hệ thống thông tin bao gồm các quy trình, thông tin liên lạc, lưu trữ và tài nguyên liên quan cần thiết cho hệ thống thông tin để hoạt động.

Ranh giới vật lý

Xác định ranh giới vật lý của một (hoặc các) hệ thống thông tin được đánh giá giới hạn phạm vi của việc đánh giá rủi ro an ninh. Một giới hạn như vậy là phù hợp theo đánh giá rủi ro an ninh nên được giới hạn đến những tài nguyên dưới sự kiểm soát của các nhà tài trợ dự án. Bên cạnh đó, một hệ thống mà không ranh giới không thể được đánh giá.

Ranh giới Logic

Xác định ranh giới logic của một (hoặc các) hệ thống thông tin được đánh giá cũng hạn chế phạm vi của đánh giá rủi ro an ninh. Một hạn chế trong phạm vi dựa trên ranh giới logic cũng là thích hợp như đánh giá rủi ro an ninh nên được giới hạn cho những chức năng hệ thống dưới sự kiểm soát của các nhà tài trợ dự án.

Mô tả dự án

Một khi dự án là đúng quy định về ngân sách, mục tiêu, sự chặt chẽ, và phạm vi, dự án cần được mô tả đúng trong hợp đồng dự án hoặc mô tả.

Các biến dự án

Mỗi biến dự án có ảnh hưởng lẫn nhau.

Các khách hàng nên quyết định thích hợp "giá trị" cho các biến dự án cho các nhu cầu của họ. Và đây là vấn đề. Nhiều khách hàng đang có được một đánh giá rủi ro an ninh từ một nhà cung cấp bên ngoài bởi vì họ không phải là chuyên

gia về an ninh thông tin và họ muốn đưa ra ý kiến bên ngoài. Vì vậy, nếu họ không phải là chuyên gia, làm sao họ có nghĩa vụ phải biết các giá trị thích hợp cho các biến dự án? Câu trả lời điển hình là " Hãy để các chuyên gia nói cho bạn. "

Trình bày công việc

Trình bày của công việc (Statement of Work: SOW) là một phần của hợp đồng quy định việc phải thực hiện. Đây có thể là đơn giản như một đoạn duy nhất hoặc phức tạp như một tài liệu nhiều trang bao gồm các kỳ vọng và giới hạn của một đánh giá rủi ro an ninh. Bất kể chiều dài hoặc phức tạp của bản thỏa thuận, nó nên ghi chép các thông số của các đánh giá rủi ro an ninh được thực hiện. Ở mức tối thiểu, các thông số này nên bao gồm các mô tả dịch vụ, phạm vi đánh giá, và mô tả của các phân phôi.

Xác định Mô tả Dịch vụ

Phạm vi điều khiển an ninh

Xác định khả năng phân phối

Loại hợp đồng

Hợp đồng Thời gian và khối lượng công việc

Hợp đồng Giá cố định

Điều khoản hợp đồng

Xác định nhu cầu

Xác định những thay thế lân cận

Thỏa thuận thành viên dự án

Chuẩn bị đánh giá rủi ro an ninh

Trước khi nhóm đánh giá nguy cơ an ninh đến nơi đánh giá tại địa điểm của khách hàng, có một số hoạt động được thực hiện để đảm bảo một dự án hiệu quả. Những hoạt động này bao gồm việc giới thiệu các nhóm đánh giá cho tổ chức, có sự cho phép để thử nghiệm và thu thập dữ liệu, và xem lại các thông tin có sẵn.

Giới thiệu Nhóm

Sự ra đời của các nhóm đánh giá nguy cơ an ninh cho các tổ chức khách hàng là quan trọng trong việc thiết lập một khởi đầu tốt cho dự án. Giới thiệu các đội đánh giá rủi ro an ninh, thông tin liên hệ, và các thông tin cá nhân của thành viên trong nhóm để các tổ chức khách hàng cung cấp sự tin cậy của khách hàng trong tính chuyên nghiệp của các nỗ lực để đi. Trong một số trường hợp, các tổ chức khách hàng có thể đã được giới thiệu với các đồng đội. Ví dụ, nhóm nghiên cứu đánh giá rủi ro an ninh có thể trình bày cho các tổ chức khách hàng trong suốt quá trình đấu thầu và đàm phán. Tuy nhiên, trong nhiều trường hợp, các thành viên của nhóm nghiên cứu đánh giá rủi ro an ninh là không biết đến các tổ chức khách hàng. Dù bằng cách nào một bức thư giới thiệu nên được sử dụng để chính thức bắt đầu các dự án đánh giá rủi ro an ninh.

Thư giới thiệu

Hình thức và nội dung của một thư giới thiệu có thể thay đổi một chút, nhưng có một số yếu tố quan trọng mà phải được chứa trong thư này. Các yếu tố chính của bức thư giới thiệu bao gồm các điểm chính của liên lạc cho cả khách hàng và các nhóm đánh giá rủi ro an ninh, một tham chiếu đến tuyên bố của công việc, một ngày bắt đầu và ngày kết thúc dự án, một ngày cho các phần trên trang web của đánh giá, yêu cầu dữ liệu tại thời điểm này, và truy cập cần thiết cho chuyến thăm trên trang web.

Pre-Assessment Briefing

Luôn luôn là tốt hơn để cho mọi người biết những gì mong đợi hơn là làm họ ngạc nhiên. Một cuộc họp báo trước đánh giá có thể giúp thiết lập những kỳ vọng của tổ chức để được đánh giá và cũng để lắng nghe mối quan tâm của họ và điều chỉnh các phương pháp đánh giá rủi ro an ninh phù hợp. Một cuộc họp báo trước đánh giá nên bao gồm các chủ đề sau:

- Giới thiệu
- Những gì để Mong đợi
    - Không phải là một thẻ Điểm mà là một công cụ lập kế hoạch
    - Bước đầu tiên trong quá trình quản lý rủi ro
    - Nhiều phát hiện
    - Không phải lúc nào cũng xử lý nhanh

- Điều mà Nhóm cần biết

Xin Giấy phép đúng

Trước khi thu thập dữ liệu, nhóm nghiên cứu đánh giá rủi ro an ninh phải được sự cho phép thích hợp cho các hoạt động thu thập dữ liệu nhất định. Những hoạt động này bao gồm giám sát của truyền thông sử dụng và truy cập vào hệ thống thông tin.

- Chính sách bắt buộc
- Giấy phép bắt buộc
- Phạm vi của Giấy phép
- Tài khoản bắt buộc

Sứ mệnh của một doanh nghiệp?

Bất cứ tổ chức nào cũng đều có lý do để tồn tại bên ngoài việc kiếm tiền. Kiếm tiền là mặt hiệu quả mong đợi của việc thực hiện sứ mệnh tốt. Đôi khi rất khó để xác định sứ mệnh doanh nghiệp. Trong một số trường hợp khác lại khá rõ ràng. Trong trường hợp của đội đánh giá rủi ro bảo mật đó là việc tìm ra câu trả lời cho 3 câu hỏi đơn giản:

• Khách hàng là ai?

• Những gì hiện tổ chức cung cấp cho khách hàng?

• Điều gì làm cho các tổ chức khác nhau từ đối thủ cạnh tranh của nó?

Đạt được thông tin sứ mạng kinh doanh

Trong phạm vi có thể, nhóm nghiên cứu đánh giá rủi ro an ninh cần phải cố gắng để có được những sứ mạng kinh doanh trước khi đến thăm tổ chức. Lướt qua các thông tin công cộng và thông tin được cung cấp có thể cho các kiến thức cần thiết để hiểu được sứ mệnh kinh doanh của tổ chức.

Xác định các hệ thống quan trọng

Các tổ chức của khách hàng có thể có nhiều hệ thống thông tin trong phạm vi của việc đánh giá rủi ro an ninh. Mỗi hệ thống quan trọng phải được xem xét một cách độc lập như họ sẽ có tài sản độc đáo, nhiệm vụ, dữ liệu, thủ tục, kiểm soát quan trọng, và chủ sở hữu dữ liệu. Một khi các hệ thống này đã được xác

định, nhóm nghiên cứu đánh giá rủi ro an ninh có thể tìm thấy một số chồng chéo giữa các hệ thống trong các điều khoản của một số khía cạnh. Ví dụ, có thể có một chủ sở hữu dữ liệu duy nhất cho hai hoặc ba hệ thống hỗ trợ một chức năng kinh doanh. Tuy nhiên, nó vẫn là quan trọng để xác định các hệ thống quan trọng cá nhân nếu có bất kỳ khía cạnh độc đáo.

Xác định mức độ quan trọng

Nhóm nghiên cứu đánh giá rủi ro an ninh nên tìm kiếm để có được một sự hiểu biết về tầm quan trọng của các hệ thống thông tin khác nhau cho sự thành công của tổ chức. Đây là một phần của sự hiểu biết sứ mệnh của tổ chức.

Xác định tài sản

Một bước quan trọng trong việc chuẩn bị cho một đánh giá rủi ro an ninh là để xác định các tài sản cần được bảo vệ. Việc xác định tài sản là một tiền chất cần thiết để hiểu được những rủi ro tổng thể đến tài sản.

Danh sách kiểm tra và đánh giá

Bảng liệt kê các tài sản dựa trên danh sách kiểm tra và đánh giá sẽ mang lại một nhận dạng đầy đủ của các tài sản quan trọng của tổ chức. Đối với nhiều người đánh giá nguy cơ an ninh này là đủ tốt, như tổ chức này sẽ là không khôn ngoan để dành toàn bộ ngân sách của mình về đánh giá rủi ro an ninh. Một nhóm nghiên cứu đánh giá rủi ro an ninh hiệu quả có thể phát triển một danh sách tương đối tốt các tài sản bằng cách xem danh sách chung về tài sản và sử dụng bản án để áp dụng danh sách để các tổ chức mà họ đang xem xét.

Phân loại tầm quan trọng/độ nhạy cảm tài sản

Tài sản là, theo định nghĩa, những vật phẩm cần được bảo vệ. Nó rất hữu ích để phân loại hoặc phân loại tài sản để tổ chức yêu cầu bảo vệ tài sản, và đánh giá tổn thương của tài sản. Có ba phương pháp tiếp cận để phân loại hoặc phân loại tài sản được mô tả dưới đây:

1. Tái sử dụng thông tin từ các đánh giá khác.
2. Xác định hệ thống quan trọng một cách nhanh chóng.
3. Xác định hệ thống quan trọng chăm.

Định giá tài sản

Một trong những bước quan trọng để thực hiện đánh giá rủi ro an ninh là xác định giá trị của tài sản cần được bảo vệ. Định giá tài sản là một yếu tố quan trọng của kế toán doanh nghiệp và lập kế hoạch trong tổ chức và có thể được thực hiện vì nhiều lý do. Những lý do này có thể bao gồm việc tuân thủ, kế hoạch dự phòng, bảo hiểm, yêu cầu pháp lý, quản lý hồ sơ, lập ngân sách, phân loại thông tin, hoặc chuyển nhượng tới hạn. Trong một đánh giá rủi ro an ninh, định giá tài sản được thực hiện để phân loại thông tin và phân công tới hạn. Định giá tài sản là một yếu tố cần thiết trong việc xác định các hệ thống quan trọng và tác động đối với tổ chức nếu tài sản bị mất hoặc bị tổn hại.

Phương pháp xác định giá trị tài sản tính

1. Đánh giá tài sản
2. Phân loại dựa trên tài sản định giá
3. Đánh giá tài sản dựa trên xếp loại
4. Định giá tài sản đồng thuận

Xác định các mối đe dọa

Các bước tiếp theo cho nhóm đánh giá rủi ro an ninh trong việc chuẩn bị cho một đánh giá rủi ro an ninh là để xác định các mối đe dọa đến hệ thống để được xem xét. Việc xác định các mối đe dọa là quan trọng bởi vì nó giáp với đánh giá để những hành động có thể được thực hiện bởi những mối đe dọa.

Thành phần của mối đe dọa

Một mối đe dọa thường được mô tả như là một sự kiện có tác động không mong muốn đối với tài sản của tổ chức. Các thành phần của một mối đe dọa bao gồm các tác nhân đe dọa và các sự kiện không mong muốn.

Tác nhân đe dọa - Threat Agent

Một tác nhân đe dọa là một thực thể có thể gây ra một mối đe dọa xảy ra, chẳng hạn như động đất hay một nhân viên bất mãn. Tác nhân đe dọa có thể được tổ chức theo kiểu của chúng (ví dụ, con người, thiên nhiên, công nghệ) và tiếp tục chia thành các loại (tức là, người trong cuộc, người ngoài, liên kết, hỏa hoạn, thời tiết, độ rung, động vật hoang dã, sinh học, cơ sở hạ tầng, hệ thống).

Sự kiện không mong muốn

Một sự kiện không mong muốn là những gì được gây ra bởi một tác nhân đe dọa. Sự kiện này được coi là không mong muốn nếu nó đe dọa một tài sản được bảo vệ. Những sự kiện này bao gồm sự phá hủy của các thiết bị, tiết lộ thông tin nhạy cảm, và thiếu nguồn lực. Sự kiện không mong muốn có thể được tổ chức theo kiểu của họ (y tế, tiếp xúc vật lý, tiếp xúc hợp lý, và nguồn lực sẵn có) và tiếp tục chia thành các tiểu thể loại (ví dụ, bệnh hoạn, gây nguy hiểm cho người, thương tật, và giết).

Liệt kê mối đe dọa có thể

Các hành động tiếp theo cho bước xác định các mối đe dọa là lên danh sách thực sự các mối đe dọa được xem xét để đánh giá rủi ro an ninh cụ thể. Trong một số trường hợp, danh sách các mối đe dọa được xem là đã có thể bị giới hạn trong giai đoạn định nghĩa dự án; Ví dụ, chỉ có các mối đe dọa bên ngoài là để được xem xét. Trong trường hợp khác, bề rộng của các mối đe dọa được coi là mở rộng. Trong cả hai trường hợp các nhóm đánh giá nguy cơ an ninh bây giờ phải xem xét sâu mà những mối đe dọa sẽ được xác định.

Phương pháp tiếp cận để liệt kê các mối đe dọa:

- Danh mục kiểm tra và đánh giá
- Hệ báo cáo mối đe doạ.

Báo cáo mối đe dọa

Thành phần mối đe dọa (tác nhân đe dọa và các sự kiện không mong muốn) có thể được kết hợp với tài sản để tạo ra báo cáo mối đe dọa. Việc tạo ra các báo cáo mối đe dọa là một cách để thể hiện rõ hơn mối đe dọa được xem xét và phản đối trong quá trình đánh giá rủi ro an ninh.

Xác định báo cáo mối đe dọa

Hành động cuối cùng cho các bước xác định các mối đe dọa là xác nhận danh sách các báo cáo mối đe dọa được phát triển trong các phần trước. Trong số các báo cáo mối đe dọa có thể được tạo ra, chỉ một phần trong số đó là đáng xem xét cho bất kỳ đánh giá rủi ro an ninh cụ thể. Xét sự phù hợp của một tuyên bố mối đe dọa phải dựa trên các mối đe dọa môi trường của tổ chức được đánh giá. Một đánh giá rủi ro an ninh cần phải có những phương pháp chứng thực chỉ có

những báo cáo mối đe dọa có vẻ như là rất có thể, bỏ qua mối đe dọa có vẻ như là một khả năng xa.

Các yếu tố ảnh hưởng đến Xác định báo cáo mối đe dọa

- Lịch sử
- Các yếu tố môi trường
- Các yếu tố kinh doanh

Xác định các điều khiển mong đợi

Bởi giai đoạn này trong đánh giá rủi ro an ninh, nhóm nên có một sự hiểu biết tốt về các mục tiêu kinh doanh, tài sản được bảo vệ, và các mối đe dọa có liên quan đến tài sản. Những thông tin này là đầy đủ để xác định các yêu cầu an ninh cao cấp cho một tổ chức. Mặc dù đánh giá rủi ro an ninh truyền thống không bao gồm một bước để phát triển các yêu cầu an ninh, kiểu phân tích này đã luôn luôn được thực hiện (có lẽ một cách vô thức) bởi nhiều chuyên gia an ninh thông tin.

Chương 3: Đáp ứng và các bước xử lý sự cố

Xử lý sự cố

Quá trình ứng phó sự cố có nhiều giai đoạn, từ khâu chuẩn bị ban đầu thông qua phân tích sau vụ việc.

Chuẩn bị

Phương pháp ứng phó sự cố thường nhấn mạnh việc chuẩn bị, không chỉ thiết lập một khả năng ứng phó sự cố để tổ chức có sẵn sàng để ứng phó sự cố, mà còn ngăn ngừa sự cố bằng cách đảm bảo rằng hệ thống, mạng, và các ứng dụng là đủ an toàn. Mặc dù đội ứng phó sự cố là không thường chịu trách nhiệm phòng ngừa sự cố, nó là rất quan trọng mà hiện nay nó được coi là một thành phần cơ bản của các chương trình ứng phó sự cố. Chuyên môn, đội phản ứng của sự cố nên có giá trị trong việc xây dựng các khuyến nghị cho việc đảm bảo hệ thống. Phần này cung cấp lời khuyên cơ bản về chuẩn bị để xử lý sự cố và phòng ngừa sự cố trên.

Chuẩn bị để xử lý sự cố

Nhiều đội ứng phó sự cố tạo ra một jump kit, một công cụ portable có chứa vật liệu mà một người xử lý sự cố có khả năng cần trong một cuộc điều tra offsite. Jump kit sẵn sàng để đi vào mọi lúc khi một sự cố nghiêm trọng xảy ra, người xử lý sự cố có thể lấy các bộ Jump và đi.

Ngăn ngừa sự cố

Giữ số sự cố hợp lý thấp là rất quan trọng để bảo vệ các quá trình kinh doanh của tổ chức. Nếu các kiểm soát an ninh là không đủ, khối lượng lớn các sự

cố có thể xảy ra, áp đảo đội ứng phó sự cố. Điều này có thể dẫn đến phản ứng chậm và không đầy đủ, mà dịch cho một tác động kinh doanh tiêu cực lớn hơn (ví dụ, thiệt hại lớn hơn, thời gian dài hơn và dịch vụ dữ liệu không có sẵn). Một cách tiếp cận âm thanh để cải thiện thế trận an ninh của tổ chức và ngăn ngừa sự cố là tiến hành đánh giá rủi ro định kỳ các hệ thống và các ứng dụng. Những đánh giá này sẽ xác định những rủi ro này được gây ra bởi sự kết hợp của các mối đe dọa và các lỗ hổng. Mỗi rủi ro cần được ưu tiên, và những rủi ro có thể được giảm nhẹ, chuyển giao, hoặc chấp nhận cho đến một mức độ tổng thể hợp lý rủi ro là đạt. Kết hợp hoặc ít nhất là kiểm tra các chiến lược kiểm soát của tổ chức chịu trách nhiệm ngang hàng có thể cung cấp sự đảm bảo hợp lý rằng những gì làm cho người khác nên làm việc cho tổ chức.

- **Patch Management**. Nhiều chuyên gia an ninh thông tin đồng ý rằng một tỷ lệ lớn các sự cố liên quan đến việc khai thác một số lượng tương đối nhỏ các lỗ hổng bảo mật trong các hệ thống và các ứng dụng. Các tổ chức lớn nên thực hiện một chương trình quản lý bản vá để hỗ trợ quản trị hệ thống trong việc xác định, thu thập, kiểm tra và triển khai các bản vá lỗi.
- **Host Security**. Tất cả các host nên cứng một cách thích hợp. Bên cạnh việc giữ mỗi host vá đúng cách, máy chủ được cấu hình để chỉ cung cấp các dịch vụ tối thiểu cho những người dùng thích hợp và host-nguyên tắc đặc quyền tối thiểu. Các thiết lập mặc định không an toàn (ví dụ, mật khẩu mặc định, cổ phiếu không có bảo đảm) phải được thay đổi. Băng rôn cảnh báo sẽ được hiển thị bất cứ khi nào người dùng cố gắng truy cập vào một nguồn lực bảo đảm. Hosts nên có kiểm toán được kích hoạt và đăng nhập nên các sự kiện bảo mật liên quan đáng kể. Nhiều tổ chức sử dụng hệ điều hành và cấu hình ứng dụng hướng dẫn để hỗ trợ quản trị trong việc đảm bảo các host thống nhất và có hiệu quả.
- **Network Security**. Các vành đai mạng nên được cấu hình để từ chối tất cả các hoạt động đó là không cho phép rõ ràng. Chỉ hoạt động cần thiết cho các hoạt động đúng đắn của các tổ chức nên được phép. Điều này bao gồm việc đảm bảo tất cả các điểm kết nối, chẳng hạn như modem, mạng riêng ảo (VPN), và các kết nối dành riêng cho các tổ chức khác.
- **Malicious Code Prevention**. Phần mềm để phát hiện và ngăn chặn mã độc hại, như virus, sâu, trojan, và mã di động độc hại, cần được triển khai toàn bộ tổ chức. Bảo vệ mã độc hại nên được triển khai ở cấp độ máy chủ (ví

dụ, máy chủ và các hệ thống điều hành máy trạm), cấp độ máy chủ ứng dụng (ví dụ, máy chủ email, Web proxy), và các ứng dụng cấp cho khách hàng (ví dụ, khách hàng email, khách hàng nhắn tin tức thời).

- **Đào tạo và nâng cao nhận thức người dùng.** Người sử dụng nên được biết về các chính sách và thủ tục liên quan đến việc sử dụng thích hợp của mạng lưới, hệ thống và các ứng dụng. Bài học áp dụng kinh nghiệm từ sự cố trước đó cũng cần được chia sẻ với người dùng để họ có thể biết hành động của họ có thể ảnh hưởng đến tổ chức. Nâng cao nhận thức người dùng về sự cố nên giảm tần số của sự cố, đặc biệt là những người liên quan đến mã độc hại và vi phạm chính sách sử dụng chấp nhận được. Công nghệ thông tin (IT) Nhân viên cần được đào tạo để họ có thể duy trì mạng lưới, hệ thống của họ, và các ứng dụng phù hợp với các tiêu chuẩn an ninh của tổ chức.

Phát hiện và phân tích

Phân loại sự cố

Sự cố có thể xảy ra theo vô số cách, vì vậy nó là không thực tế để xây dựng quy trình toàn diện với hướng dẫn step - by - step để xử lý mọi sự cố. Việc tốt nhất mà tổ chức có thể làm là để chuẩn bị chung để xử lý bất kỳ loại sự cố và cụ thể hơn để xử lý các loại sự cố thông thường. Các loại sự cố được liệt kê dưới đây là không toàn diện cũng không có ý định để cung cấp phân loại dứt khoát cho sự cố; thay vào đó, họ chỉ cần cung cấp một cơ sở để cung cấp lời khuyên về làm thế nào để xử lý sự cố dựa trên thể loại chính của họ:

- Denial of Service
- Malicious Code
- Unauthorized Access
- Inappropriate Usage
- Multiple Component

Một số sự cố có thể thuộcvào nhiều hơn 1 loại.

Dấu hiệu của một sự cố

Đối với nhiều tổ chức, công đoạn khó khăn nhất của quá trình ứng phó sự cố được phát hiện một cách chính xác và đánh giá sự cố có thể-xác định xem sự cố đã xảy ra, và nếu như vậy, loại hình, mức độ, và độ lớn của vấn đề.

Dấu hiệu của một sự cố rơi vào một trong hai loại: những chỉ dẫn và người đi trước.Một số ví dụ được liệt kê dưới đây:

- Các cảnh báo cảm biến phát hiện xâm nhập mạng khi một cố gắng tràn bộ đệm xảy ra đối với một máy chủ FTP.
- Các cảnh báo phần mềm diệt virus khi nó phát hiện rằng một máy chủ bị nhiễm một con sâu.
- Những tai nạn máy chủ Web.
- Người dùng phàn nàn về sự chậm truy cập vào máy chủ trên Internet.
- Quản trị hệ thống nhìn thấy một tên tập tin với các nhân vật khác thường.
- Những người sử dụng gọi các trợ giúp để có báo cáo một tin nhắn email đe dọa.
- Các máy chủ ghi lại một sự thay đổi cấu hình kiểm toán trong nhật ký của mình.
- Các bản ghi ứng dụng nhiều thất bại trong nỗ lực đăng nhập từ một hệ thống từ xa không quen thuộc.
- Người quản trị email thấy một số lượng lớn các email bị trả về với nội dung đáng ngờ.
- Người quản trị mạng thấy có một độ lệch bất thường từ các luồng lưu lượng mạng điển hình.

Nguồn từ người đi trước và chỉ dẫn

Người đi trước và chỉ dẫn được xác định bằng cách sử dụng nhiều nguồn khác nhau, với các cảnh báo được phổ biến hầu hết các phần mềm bảo mật máy tính, các bản ghi, thông tin công khai, và con người.

Phân tích sự cố

Phát hiện và phân tích sự cố sẽ dễ dàng nếu mỗi người đi trước hoặc chỉ dẫn được bảo đảm là chính xác; nhưng không may, nó thường không phải như vậy.

Hệ thống phát hiện xâm nhập được nổi tiếng vì sản xuất số lượng lớn lỗi đúng - sai chỉ dẫn.

Ngay cả khi một dấu hiệu cho thấy là chính xác, nó không nhất thiết có nghĩa là một sự cố đã xảy ra. Một số dấu hiệu, chẳng hạn như một vụ tai nạn máy chủ Web hoặc sửa đổi các tập tin quan trọng, có thể xảy ra vì nhiều lý do khác hơn là một sự cố an ninh, bao gồm cả lỗi của con người.

Một số sự cố dễ dàng để phát hiện, chẳng hạn như một trang web bị thay đổi nội dung. Tuy nhiên, nhiều sự cố không liên quan đến các triệu chứng rõ ràng như vậy. Dấu hiệu nhỏ như một sự thay đổi trong một tập tin cấu hình hệ thống có thể là dấu hiệu cho thấy rằng chỉ có một sự cố đã xảy ra. Trong xử lý sự cố, phát hiện có thể là nhiệm vụ khó khăn nhất. Xử lý sự cố là trách nhiệm phân tích mơ hồ, mâu thuẫn, và các triệu chứng không đầy đủ để xác định những gì đã xảy ra. Mặc dù các giải pháp kỹ thuật tồn tại mà có thể làm cho việc phát hiện phần nào dễ dàng hơn, các biện pháp khắc phục tốt nhất là xây dựng một đội ngũ giàu kinh nghiệm và thành thạo cán bộ nhân viên có thể phân tích các tiền chất và chỉ có hiệu quả và có hiệu quả và có những hành động thích hợp. Nếu không có một đội ngũ nhân viên được đào tạo và có khả năng, phát hiện và phân tích vụ việc sẽ được tiến hành không có hiệu quả, và những sai lầm tốn kém sẽ được thực hiện.

Các đội phản ứng sự cố nên làm việc một cách nhanh chóng để phân tích và xác nhận từng sự việc, tài liệu từng bước thực hiện. Khi nhóm nghiên cứu tin rằng một sự cố đã xảy ra, nhóm nghiên cứu nhanh chóng nên thực hiện một phân tích ban đầu để xác định phạm vi của vụ việc, chẳng hạn như các mạng, hệ thống, hoặc các ứng dụng bị ảnh hưởng; ai hay cái gì có nguồn gốc vụ việc; và làm thế nào sự việc đang xảy ra (ví dụ, những công cụ hay phương pháp tấn công đang được sử dụng, những lỗ hổng được khai thác). Những phân tích ban đầu sẽ cung cấp đủ thông tin cho đội tuyển để ưu tiên các hoạt động tiếp theo, chẳng hạn như ngăn chặn các vụ việc và phân tích sâu sắc hơn về những ảnh hưởng của sự cố. Khi nghi ngờ, xử lý sự cố nên giả tồi tệ nhất cho đến khi phân tích thêm chỉ khác.

Thực hiện phân tích ban đầu và xác nhận là một thách thức. Các khuyến nghị sau đây để làm phân tích sự cố dễ dàng hơn và hiệu quả hơn:

- Hồ sơ hóa hệ thống và mạngProfile
- Hiểu các hành vi thông thương
- Sử dụng tập trung hóa logging và chính sách duy trì log

- Thực hiện các sự kiện tương quan
- Đồng bộ tất cả đồng hồ của các host
- Sử dụng và duy trì kiến thức cơ bản về thông tin
- Sử dụng các công cụ tìm kiếm trên internet để nghiên cứu
- Thực thi Packet Sniffers để thu thập thêm thông tin
- Xem xét việc lọc dữ liệu
- Xem xét các trải nghiệm là không thể thay thế
- Tạo một ma trận chẩn đoán cho các nhân viên ít kinh nghiệm
- Tìm kiếm sự hỗ trợ từ người khác

Văn bản sự cố

Ngay sau khi một đội phản ứng sự cố nghi ngờ rằng một sự cố đang xảy ra hoặc đã xảy ra, điều quan trọng là ngay lập tức bắt đầu ghi tất cả các sự kiện liên quan đến vụ việc. Ghi sự kiện hệ thống, các cuộc trò chuyện qua điện thoại, và những thay đổi quan sát thấy trong các tập tin có thể dẫn đến việc xử lý hiệu quả hơn, hệ thống hơn, và ít bị lỗi. Mỗi bước được thực hiện từ thời điểm vụ việc được phát hiện đến giải pháp cuối cùng phải được ghi chép và ghi lại ngày tháng. Mỗi tài liệu liên quan đến vụ việc nên được ghi ngày tháng và chữ ký của người xử lý sự cố. Thông tin có tính chất này cũng có thể được sử dụng làm bằng chứng tại tòa án của pháp luật nếu bị truy tố theo đuổi. Bất cứ khi nào có thể, người xử lý nên làm việc trong đội với ít nhất hai người: một người có thể ghi lại và log các sự kiện trong khi người khác thực hiện các nhiệm vụ kỹ thuật.

Các đội phản ứng sự cố nên giữ hồ sơ về tình trạng sự cố, cùng với thông tin cần thiết khác. Sử dụng một ứng dụng hoặc một cơ sở dữ liệu cho mục đích này là cần thiết để đảm bảo rằng sự cố được xử lý và giải quyết một cách kịp thời. Việc xử lý có thể nhanh chóng trở nên quen thuộc với sự việc bằng cách truy cập cơ sở dữ liệu sự cố, mà nên chứa thông tin về những điều sau đây:

- Tình trạng hiện tại của vụ việc
- Một bản tóm tắt về vụ việc
- Hành động của tất cả các xử lý sự cố về sự cố này
- Thông tin liên lạc cho các bên liên quan khác (ví dụ, chủ sở hữu hệ thống, quản trị hệ thống)
- Một danh sách các bằng chứng thu thập được trong cuộc điều tra vụ việc

- Ý kiến từ xử lý sự cố
- Các bước tiếp theo sẽ được thực hiện (ví dụ, chờ đợi một người quản trị hệ thống để vá một ứng dụng).

Phân cấp mức độ ưu tiên sự cố

Thực hiện theo ưu tiên việc xử lý các vụ việc có lẽ là thời điểm quyết định quan trọng nhất trong quá trình xử lý sự cố. Sự cố không nên được xử lý dạng đơn giản xảy ra trước xử lý trước như là một kết quả của những hạn chế về nguồn lực. Thay vào đó, việc xử lý cần được ưu tiên dựa trên hai yếu tố:

- Ảnh hưởng kỹ thuật tại thời điểm hiện tại và tiềm năng của sự cố
- Mức độ quan trọng của các tài nguyên bị tác động

Thông báo sự cố

Khi một sự cố được phân tích và ưu tiên, các đội phản ứng sự cố cần phải thông báo cho các cá nhân thích hợp trong tổ chức và, đôi khi, các tổ chức khác. Báo cáo kịp thời và thông báo cho phép tất cả những người cần phải được tham gia đóng vai trò của họ. Các yêu cầu báo cáo chính xác khác nhau giữa các cơ quan, nhưng các bên được thông báo thường bao gồm-

- Giám đốc công nghệ thông tin - CIO
- Trưởng bộ phận An toàn an ninh thông tin
- Các nhân viên ATANTT cục bộ
- Các nhóm đáp ứng sự cố khác trong tổ chức
- Chủ sở hữu hệ thống
- Bộ phận nhân sự
- Thông báo rộng rãi (đối với những sự cố có thể công khai)
- Phòng phụ trách về luật (đối với các sự cố có liên quan pháp luật)
- Đơn vị ứng cứu sự cố khẩn cấp (theo quy định của từng chính phủ)

Phương pháp truyền thông có thể bao gồm-

- Email
- Web site (Intranet-based)
- Gọi điện
- Trực tiếp

- Thông báo qua Voice mailbox
- Văn bản (ví dụ, dán thông báo ở bảng tin…).

Ngăn chặn, xoá, và phục hồi

Lựa chọn chiến lượng ngăn chặn

Khi một sự cố đã được phát hiện và phân tích, điều quan trọng là để ngăn chặn nó trước sự lây lan của vụ việc lấn át tài nguyên hoặc tăng thiệt hại. Hầu hết các sự cố cần ngăn chặn, vì vậy điều quan trọng là phải xem xét nó sớm trong quá trình xử lý từng vụ việc. Một phần quan trọng của ngăn chặn là ra quyết định (ví dụ, tắt hệ thống, ngắt kết nối từ mạng có dây hoặc không dây, ngắt kết nối modem cáp của mình, xóa chức năng nhất định). Quyết định đó là dễ dàng hơn nhiều để thực hiện nếu các chiến lược và thủ tục có chứa sự việc đã được xác định trước. Tổ chức phải xác định rủi ro chấp nhận được trong việc đối phó với các sự cố và phát triển các chiến lược phù hợp.

Chiến lược ngăn chặn khác nhau dựa trên các loại của sự cố. Là rất khuyến khích các tổ chức tạo ra các chiến lược ngăn riêng biệt cho từng loại chính của sự cố. Các tiêu chí cần được ghi chép rõ ràng để tạo thuận lợi cho việc ra quyết định nhanh chóng và hiệu quả. Tiêu chí xác định các chiến lược thích hợp bao gồm:

- Thiệt hại tiềm tàng đến và trộm cắp tài nguyên
- Cần bảo quản bằng chứng
- Dịch vụ sẵn có (ví dụ, kết nối mạng, dịch vụ cung cấp cho bên ngoài)
- Thời gian và nguồn lực cần thiết để thực hiện chiến lược
- Hiệu quả của chiến lược (ví dụ, một phần có chứa vụ việc, hoàn toàn có sự cố)
- Thời hạn của giải pháp (ví dụ, cách giải quyết trường hợp khẩn cấp phải được loại bỏ trong bốn giờ, cách giải quyết tạm thời được loại bỏ trong hai tuần, giải pháp lâu dài).

Thu thập bằng chứng và xử lý

Mặc dù lý do chính để thu thập bằng chứng trong một vụ việc là để giải quyết vụ việc, nó cũng có thể cần thiết cho thủ tục tố tụng pháp lý. Trong trường hợp này, điều quan trọng là tài liệu rõ ràng cách tất cả các bằng chứng, bao gồm cả hệ thống bị xâm nhập, đã được bảo quản. Bằng chứng cần được thu thập theo

thủ tục đáp ứng tất cả các luật và quy định, phát triển từ các cuộc thảo luận trước với nhân viên pháp lý và các cơ quan thực thi pháp luật phù hợp, do đó nó phải được chấp nhận tại tòa án. Ngoài ra, bằng chứng phải được hạch toán theo mọi lúc; bất cứ khi nào bằng chứng được chuyển từ người này sang người khác, chuỗi các hình thức giam giữ nên cụ thể việc chuyển giao và có chữ ký của mỗi bên. Một bản ghi chi tiết phải được giữ cho tất cả các bằng chứng, bao gồm những điều sau đây:

- Xác định thông tin (ví dụ, vị trí, số serial, số mô hình, tên máy, kiểm soát truy cập media (MAC address) và địa chỉ IP của một máy tính)
- Tên, số danh hiệu, và điện thoại của mỗi cá nhân được thu thập hoặc xử lý các bằng chứng trong cuộc điều tra
- Thời gian và ngày tháng (bao gồm cả vùng thời gian) của mỗi sự xuất hiện của các chứng cứ xử lý
- Địa điểm nơi các chứng cứ đã được lưu trữ.

Xác định kẻ tấn công

Trong thời gian xử lý sự cố, chủ hệ thống và những người khác thường muốn để xác định kẻ tấn công. Mặc dù thông tin này có thể quan trọng, đặc biệt là nếu tổ chức muốn truy tố những kẻ tấn công, người xử lý sự cố nên tiếp tục tập trung vào ngăn chặn, xóa, và phục hồi. Xác định kẻ tấn công có thể là tiến trình tốn một thời gian lớn và vô ích và có thể ngăn chặn nhóm khỏi việc đạt được mục tiêu giảm thiểu các tác động kinh doanh chính của nó. Các mục sau đây mô tả các hoạt động phổ biến nhất được thực hiện để xác định kẻ tấn công:

- Xác nhận tính hợp lệ địa chỉ IP của kẻ tấn công
- Quét hệ thống của kẻ tấn công
- Nghiên cứu kẻ tấn công thông qua các bộ công cụ tìm kiếm
- Sử dụng cơ sở dữ liệu sự cố
- Giám sát các kênh truyền thông có thể của kẻ tấn công

Xóa và Khôi phục

Sau khi một sự cố đã được ngăn chặn, việc xóa có thể cần thiết để loại bỏ các thành phần của vụ việc, chẳng hạn như xóa mã độc hại và vô hiệu hóa tài

khoản người dùng bị vi phạm. Đối với một số sự cố, việc xoá hoặc là không cần thiết hoặc được thực hiện trong quá trình phục hồi.

Trong phục hồi, các quản trị viên hệ thống khôi phục lại hoạt động bình thường và (nếu có) gia cố hệ thống để ngăn chặn sự cố tương tự. Phục hồi có liên quan đến hành động như khôi phục lại từ bản sao lưu hệ thống sạch, xây dựng lại hệ thống từ đầu, thay thế các file bị xâm nhập với các phiên bản sạch, cài đặt các bản vá lỗi, thay đổi mật khẩu, và thắt chặt mạng vành đai an ninh

Khi một tài nguyên bị tấn công thành công, nó thường bị tấn công một lần nữa, hoặc các nguồn lực khác trong tổ chức bị tấn công theo cách tương tự. Nhiều nguồn tài nguyên có giá trị có sẵn trên mạng Internet để phục hồi và bảo vệ hệ thống Bởi vì xóa và phục hồi các hành động được hệ thống (hệ điều hành) hoặc ứng dụng cụ thể, đề xuất chi tiết và tư vấn điển hình hoạt động liên quan đến họ nằm ngoài phạm vi của tài liệu này.

Hành động sau sự cố

Rút ra bài học kinh nghiệm

Một trong những phần quan trọng nhất của phản ứng sự cố cũng thường bị bỏ qua: học tập và cải thiện. Mỗi đội ứng phó sự cố nên phát triển để phản ánh các mối đe dọa mới, cải tiến công nghệ, và bài học kinh nghiệm. Nhiều tổ chức đã tìm thấy rằng việc tổ chức một cuộc họp "bài học kinh nghiệm" với tất cả các bên liên quan sau khi một sự cố lớn, và định kỳ sau khi sự cố thấp hơn, là vô cùng hữu ích trong việc cải thiện các biện pháp an ninh và xử lý sự cố tiến trình chính nó. Cuộc họp này cung cấp một cơ hội để đạt được việc đóng lại đối với một sự cố bằng cách xem xét những gì xảy ra, những gì đã được thực hiện để can thiệp, và cách can thiệp cũng làm việc. Cuộc họp sẽ được tổ chức trong những ngày cuối của vụ việc. Câu hỏi để được trả lời trong các bài học kinh nghiệm đáp ứng bao gồm:

- Xác định chính xác cái gì đã xảy ra và vào lúc nào?
- Nhân viên xử lý tốt đến mức nào trong việc giải quyết sự cố đó?
- Nó có theo các thủ tục văn bản không?
- Họ làm đúng thẩm quyền không?
- Thông tin gì cần sớm hơn?

- Có bước hay hành động nào đã xảy ra làm hạn chế việc khôi phục?
- Nhân viên và quản lý có thể làm khác không nếu sự cố tương tự lại xảy ra?
- Những hành động khắc phục nào có thể ngăn chặn các sự cố tương tự trong tương lai?
- Những công cụ và tài nguyên nào cần thêm để phát hiện, phân tích và giảm các sự cố trong tương lai?

Sử dụng các dữ liệu sự cố thu được

Bài học kinh nghiệm hoạt động nên tạo ra một tập hợp các dữ liệu khách quan và chủ quan đối với từng vụ việc. Theo thời gian, các dữ liệu sự cố thu thập trở nên hữu ích trong một số năng lực. Các dữ liệu, đặc biệt là tổng số giờ tham gia và các chi phí, có thể được sử dụng để biện minh cho việc bổ sung kinh phí của đội ứng phó sự cố. Một nghiên cứu về đặc điểm sự cố có thể chỉ ra điểm yếu của hệ thống an ninh và các mối đe dọa, cũng như những thay đổi trong xu hướng cố. Dữ liệu này có thể được đưa trở lại vào quá trình đánh giá rủi ro, cuối cùng dẫn đến việc lựa chọn và thực hiện các điều khiển bổ sung. Nếu dữ liệu sự cố được thu thập và lưu trữ đúng cách, nó sẽ cung cấp một số biện pháp của sự thành công (hoặc ít nhất là các hoạt động) của đội ứng phó sự cố. Hơn nữa, các tổ chức đó được yêu cầu phải báo cáo thông tin sự cố sẽ cần phải thu thập các dữ liệu cần thiết để đáp ứng yêu cầu của họ.

Tham số đánh gia cho sự cố liên quan đến dữ liệu bao gồm-

- Số lượng xử lý sự cố
- Thời gian cho mỗi sự cố
    - Tổng số nhân lực phải bỏ ra làm việc về vụ việc
    - Tổng thời gian từ khi bắt đầu xảy ra sự việc đến giải quyết nó
    - Tổng thời gian cho từng giai đoạn của quá trình xử lý sự cố (ví dụ, ngăn chặn, phục hồi)
    - Mất bao lâu đội ứng phó sự cố phản hồi về báo cáo nguyên nhân gốc của vụ việc.
    - Mất bao lâu để báo cáo sự việc cho quản lý và, nếu cần thiết, với đơn vị bên ngoài thích hợp (ví dụ, US-CERT).
- Đánh giá khách quan của mỗi sự cố

- Đánh giá chủ quan mỗi sự cố

Lưu giữ bằng chứng

Tổ chức phải thiết lập các chính sách cho việc lưu trữ bao lâu và thế nào các bằng chứng từ một sự cố. Hầu hết các tổ chức lựa chọn để giữ lại tất cả các bằng chứng trong nhiều tháng hoặc nhiều năm sau khi vụ việc kết thúc. Các yếu tố sau đây cần được xem xét trong quá trình tạo chính sách:

- Truy tố
- Lưu trữ dữ liệu
- Chi phí

Bảng kê công việc xử lý sự cố

Bảng kê cung cấp các bước chính để thực hiện việc xử lý ban đầu của một sự cố. Những khái niệm chỉ xác định trong việc phát hiện và phân tích một sự cố; sau khi bảng kê này được hoàn thành, người xử lý sự cố sẽ dùng bảng này để hướng đến loại hình cụ thể của sự cố.

Ví dụ về bảng kê xử lý sự cố

	Action	Completed
Detection and Analysis		
1.	Determine whether an incident has occurred	
1.1	Analyze the precursors and indications	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence	
2.	Classify the incident using the categories (e.g., denial of service, malicious code, unauthorized access, inappropriate usage, multiple component)	

3.	Follow the appropriate incident category checklist; if the incident does not fit into any of the categories, follow the generic checklist	

Khuyến nghị

Các khuyến nghị chính được trình bày trong phần này để xử lý sự cố được tóm tắt dưới đây.

- **Phải có các công cụ và nguồn lực có thể có giá trị trong quá trình xử lý sự cố**. Đội phản ứng sẽ có hiệu quả hơn trong việc đối sự cố nếu các công cụ khác nhau và các nguồn lực đã có sẵn cho họ. Ví dụ như danh sách liên lạc, phần mềm mã hóa, sơ đồ mạng, các thiết bị sao lưu, phần mềm máy tính pháp y, danh sách cảng, và các bản vá lỗi bảo mật.
- **Ngăn chặn sự cố xảy ra bằng cách đảm bảo rằng các mạng lưới, hệ thống và các ứng dụng là đủ an toàn.** Ngăn chặn sự cố là có lợi cho tổ chức và cũng làm giảm khối lượng công việc của đội ứng phó sự cố. Thực hiện đánh giá rủi ro định kỳ và giảm các rủi ro được xác định ở mức chấp nhận được hiệu quả trong việc giảm số lượng các sự cố. Người sử dụng, nhân viên IT, quản lý và nhận thức về chính sách và thủ tục an ninh cũng rất quan trọng.
- **Xác định những người đi trước và các chỉ dẫn thông qua các cảnh báo được tạo ra bởi vài loại phần mềm bảo mật máy tính.** Phát hiện xâm nhập và phòng chống các hệ thống, phần mềm antivirus và antispyware, và tính toàn vẹn file phần mềm kiểm tra có giá trị để phát hiện dấu hiệu sự cố. Mỗi loại phần mềm có thể phát hiện sự cố mà các loại phần mềm có thể không, vì vậy việc sử dụng của một số loại phần mềm bảo mật máy tính là rất khuyến khích. Dịch vụ giám sát của bên thứ ba cũng có thể hữu ích.
- **Thiết lập các cơ chế cho đối tác bên ngoài để báo cáo sự cố**. Bên ngoài có thể muốn báo cáo sự cố cho tổ chức; Ví dụ, họ có thể tin rằng một số người dùng của tổ chức tấn công họ. Các tổ chức nên công bố một số điện thoại và địa chỉ email mà bên ngoài có thể sử dụng để báo cáo sự cố như vậy.
- **Yêu cầu một mức độ baseline về bản log và kiểm soát trên tất cả các hệ thống, và một mức độ baseline cao hơn trên tất cả các hệ thống quan trọng**. Logs từ hệ điều hành, dịch vụ và ứng dụng thường xuyên cung cấp

các giá trị trong khi phân tích sự cố, đặc biệt là nếu kiểm toán đã được kích hoạt. Các bản ghi có thể cung cấp thông tin như các tài khoản đã truy cập và những hành động được thực hiện.

- **Hồ sơ các mạng và hệ thống**. Việc hồ sơ hóa xác định đặc điểm của mức độ hoạt động dự kiến để thay đổi trong mô hình có thể được xác định dễ dàng hơn. Nếu quá trình hồ sơ hóa là tự động, độ lệch từ mức độ hoạt động dự kiến có thể được phát hiện và báo cáo cho quản trị viên một cách nhanh chóng, dẫn đến việc phát hiện nhanh các sự cố và các vấn đề hoạt động.
- **Hiểu về các hành vi bình thường của mạng lưới, hệ thống và các ứng dụng**. Thành viên trong nhóm, là những người hiểu hành vi bình thường nên có thể nhận ra hành vi bất thường dễ dàng hơn. Kiến thức này tốt nhất có thể đạt được bằng cách xem xét các mục log và cảnh báo an ninh; các bộ xử lý trở nên quen thuộc với các dữ liệu điển hình và có thể điều tra các mục khác thường để đạt được kiến thức nhiều hơn nữa.
- **Sử dụng nhật ký tập trung và tạo ra một chính sách duy trì log**. Thông tin liên quan đến một sự cố có thể được ghi nhận ở một vài nơi. Các tổ chức nên triển khai máy chủ nhật ký tập trung và cấu hình thiết bị để gửi bản sao các mục đăng nhập của họ đến các máy chủ tập trung. Những lợi ích đội bóng bởi vì nó có thể truy cập vào tất cả các mục đăng nhập cùng một lúc; cũng có thể, những thay đổi được thực hiện cho các bản ghi trên máy cá nhân sẽ không ảnh hưởng đến dữ liệu đã được gửi đến các máy chủ tập trung. Một chính sách duy trì đăng nhập là quan trọng bởi vì các mục nhật ký cũ có thể cho thấy các trường hợp trước đây hoạt động tương tự hoặc có liên quan.
- **Thực hiện các sự kiện tương quan**. Chỉ dẫn của một sự cố có thể được chụp trong một số bản ghi. Tương quan giữa các sự kiện nhiều nguồn có thể là vô giá trong việc thu thập tất cả các thông tin có sẵn cho một sự cố và xác nhận cho dù sự việc xảy ra. Trung khai thác gỗ làm cho sự kiện tương quan dễ dàng hơn và nhanh hơn.
- **Giữ tất cả các đồng hồ đồng bộ**. Nếu các thiết bị báo cáo các sự kiện có các cài đặt đồng hồ không nhất quán, sự kiện tương quan sẽ phức tạp hơn. Sai lệch đồng hồ cũng có thể gây ra các vấn đề từ một quan điểm chứng cứ.
- **Duy trì và sử dụng một cơ sở tri thức của thông tin**. Xử lý cần phải tham khảo thông tin một cách nhanh chóng trong khi phân tích sự cố; một cơ sở

tri thức tập trung cung cấp một nguồn duy trì nhất quán của thông tin. Các kiến thức cơ bản nên bao gồm thông tin chung, chẳng hạn như số cổng thường được sử dụng và các liên kết đến thông tin phần mềm độc hại, cũng như số liệu về tiền chất và các dấu hiệu của sự cố trước đó.

- **Tạo một ma trận chẩn đoán cho nhân viên ít kinh nghiệm**. Trợ giúp nhân viên bàn, quản trị hệ thống, và các thành viên đội ứng phó sự cố mới có thể cần hỗ trợ trong việc xác định những loại sự cố có thể xảy ra. Một ma trận chẩn đoán liệt kê loại sự cố và các triệu chứng liên quan với mỗi loại có thể cung cấp lời khuyên về những gì loại của sự cố đang xảy ra và cách thức biến cố có thể được xác nhận.
- **Bắt đầu ghi lại tất cả thông tin ngay sau khi đội nghi ngờ rằng một sự cố đã xảy ra**. Mỗi bước thực hiện, kể từ thời điểm vụ việc đã được phát hiện để giải quyết cuối cùng của nó, nên được ghi chép và ghi lại. Thông tin của thiên nhiên này có thể phục vụ như là bằng chứng tại tòa án của pháp luật nếu bị truy tố theo đuổi. Việc ghi lại các bước thực hiện cũng có thể dẫn đến một xử lý dễ bị lỗi hiệu quả hơn và có hệ thống, và ít hơn của vấn đề.
- **Bảo vệ dữ liệu sự cố**. Nó thường chứa thông tin nhạy cảm liên quan đến những thứ như các lỗ hổng, lỗ hổng bảo mật, và người dùng có thể thực hiện những hành động không phù hợp. Các đội phải đảm bảo rằng quyền truy cập vào dữ liệu sự cố bị hạn chế đúng cách, cả hợp lý và thể chất.
- **Ưu tiên hóa các sự cố theo tác động kinh doanh trên cơ sở độ quan trọng của các nguồn tài nguyên bị ảnh hưởng và hiệu quả kỹ thuật của sự cố**. Do hạn chế của tài nguyên, sự cố không nên được xử lý dạng xảy ra trước – xử lý trước. Thay vào đó, các tổ chức cần thiết lập các hướng dẫn bằng văn bản phác họa như thế nào một cách nhanh chóng các đội phải ứng phó sự cố và những hành động cần được thực hiện, dựa trên tác động kinh doanh hiện tại và tiềm năng của sự cố. Điều này tiết kiệm thời gian cho các trình xử lý sự cố và cung cấp một sự biện minh để quản lý và hệ thống chủ cho hành động của họ. Các tổ chức cũng nên thiết lập một quá trình leo thang đối với những trường hợp khi đội bóng không đáp ứng với một sự cố trong thời gian được chỉ định.
- **Đưa các quy định về báo cáo sự cố vào trong chính sách ứng phó sự cố của tổ chức**. Các tổ chức nên xác định những sự cố phải được báo cáo, khi

họ phải được báo cáo, và cho ai. Các bên thường được thông báo là các CIO, người đứng đầu an ninh thông tin, địa phương nhân viên an ninh thông tin, các đội ứng phó sự cố khác trong tổ chức, và chủ sở hữu của hệ thống.

- **Xây dựng chiến lược và thủ tục có chứa sự cố**. Điều quan trọng là phải có sự cố một cách nhanh chóng và hiệu quả để hạn chế tác động kinh doanh của họ. Tổ chức phải xác định những rủi ro có thể chấp nhận trong việc kiềm cố và phát triển các chiến lược và quy trình cho phù hợp. Chiến lược ngăn chặn nên khác nhau dựa trên các loại của sự cố.
- **Thực hiện theo các thủ tục đã thiết lập để thu thập bằng chứng và xử lý**. Các đội phải ghi rõ ràng như thế nào tất cả các bằng chứng đã được bảo tồn. Bằng chứng phải được hạch toán theo tất cả các lần. Các đội phải đáp ứng với các nhân viên thực thi pháp luật và cơ quan pháp luật để thảo luận về việc xử lý chứng cứ, sau đó phát triển các thủ tục dựa trên những cuộc thảo luận.
- **Chụp dữ liệu tạm thời từ các hệ thống làm bằng chứng**. Điều này bao gồm danh sách các kết nối mạng, các quy trình, các phiên đăng nhập, mở tập tin, cấu hình giao diện mạng, và các nội dung của bộ nhớ. Chạy các lệnh chọn lựa cẩn thận từ phương tiện truyền thông đáng tin cậy có thể thu thập các thông tin cần thiết mà không gây tổn hại bằng chứng của hệ thống.
- **Lấy ảnh chụp nhanh hệ thống thông qua đầy đủ các hình ảnh đĩa pháp y, không qua bản sao lưu hệ thống**. Ảnh đĩa nên được thực hiện để làm vệ sinh phương tiện truyền thông ghi-bảo hộ hoặc ghi một lần. Quá trình này là cao với một bản sao lưu hệ thống tập tin cho các mục đích điều tra và bằng chứng. Imaging cũng rất có giá trị ở chỗ nó là an toàn hơn nhiều để phân tích một hình ảnh hơn là để thực hiện các phân tích trên hệ thống ban đầu vì các phân tích có thể vô tình làm thay đổi bản gốc.
- **Giữ các bài học kinh nghiệp gặp phải sau các sự cố lớn**. Bài học kinh nghiệm này là cực kỳ hữu ích trong việc cải thiện các biện pháp an ninh và xử lý sự cố tiến trình chính nó.

Chương 4: Xử lý các sự cố an ninh mạng

Thu thập các bằng chứng trên mạng

Chúng ta sẽ xem xét làm thế nào để tập hợp một hệ thống giám sát mạng mạnh, an toàn và theo dõi được toàn bộ nội dung giám sát lưu lượng mạng

Bằng chứng dựa trên mạng là gì?

Chúng ta coi kết quả củ việc giám sát toàn bộ nội dung mạng hoặc sự can thiệp của các truyền thông điện tử là bằng chứng dựa trên mạng - *network-based evidence*. Thu thập chứng cứ dựa trên mạng bao gồm việc thiết lập một hệ thống máy tính để thực hiện giám sát mạng, triển khai mạng lưới giám sát và đánh giá hiệu quả của mạng lưới giám sát.

Nắm bắt các lưu lượng truy cập chỉ là một phần của công trình; chiết xuất kết quả có ý nghĩa là thách thức khác. Sau khi bạn đã thu thập các dữ liệu thô mà sáng tác bằng chứng networkbased của bạn, bạn phải phân tích dữ liệu đó. Việc phân tích các bằng chứng dựa trên mạng bao gồm xây dựng lại mạng lưới hoạt động, thực hiện phân tích giao thức cấp thấp, và giải thích các hoạt động mạng.

Các mục tiêu của giám sát mạng là gì?

Nếu một nhân viên thực thi pháp luật nghi ngờ một cá nhân của một tội phạm như buôn bán ma túy nhỏ, nghi ngờ thường được đặt dưới sự giám sát để xác nhận mối nghi ngờ, tích lũy bằng chứng, và xác định đồng phạm. Các phương pháp tiếp cận giống như vậy với các tội phạm bị nghi ngờ chống lại các mạng máy tính. Mạng lưới giám sát không có ý định để ngăn chặn các cuộc tấn công. Thay vào đó, nó cho phép các nhà điều tra để thực hiện một số nhiệm vụ:

- Xác nhận hoặc xua tan những nghi ngờ xung quanh một sự cố an ninh máy tính bị cáo buộc.
- Tích lũy bằng chứng và thông tin bổ sung.
- Kiểm tra phạm vi của một thỏa hiệp.
- Xác định các bên tham gia thêm.

- Xác định thời gian của các sự kiện xảy ra trên mạng.
- Bảo đảm sự phù hợp với hoạt động mong muốn.

Các loại giám sát mạng

Giám sát mạng có thể bao gồm nhiều loại khác nhau của bộ sưu tập dữ liệu: theo dõi sự kiện, theo dõi bẫy và dấu vết, và theo dõi đầy đủ nội dung. Khi ứng phó sự cố an ninh máy tính, bạn sẽ có khả năng dựa vào việc thu thập dữ liệu đầy đủ nội dung với các công cụ như tcpdump. Tuy nhiên, có thể có những lúc bạn sẽ chặn hoàn toàn các dữ liệu giao dịch với một cái trap-and-trace.

Giám sát sự kiện

Giám sát sự kiện dựa trên các quy tắc hoặc ngưỡng sử dụng trên nền tảng giám sát mạng. Các sự kiện chỉ đơn giản là cảnh báo rằng một cái gì đó xảy ra trên mạng của bạn. Sự kiện truyền thống được tạo ra bởi một mạng IDS, nhưng sự kiện này cũng có thể được tạo ra bởi phần mềm mạng theo dõi sức khỏe như MRTG (Multi Router Traffic Grapher) hoặc NTOP.

Giám sát Trap-and-Trace

Giám sát không nội dung ghi lại phiên, giao dịch dữ liệu tổng kết các hoạt động mạng. Về mặt pháp luật coi giám sát không nội dung như một *pen register* or a *trap-and-trace*. Nó thường bao gồm các giao thức, địa chỉ IP, và các cổng được sử dụng bởi một mạng truyền thông. Số liệu bổ sung có thể bao gồm các cờ nhìn thấy trong cuộc hội thoại (nếu TCP được sử dụng), đếm số lượng các byte của thông tin được gửi bởi mỗi bên, và số lượng của các gói dữ liệu được gửi bởi mỗi bên.

Giám sát toàn bộ nội dung

Giám sát toàn bộ nội dungtạo ra dữ liệu bao gồm các gói dữ liệu thô được thu thập từ đường truyền. Nó cung cấp độ trung thực cao nhất, bởi vì nó thể hiện sự giao tiếp thực tế thông qua giữa các máy tính trên mạng. Dữ liệu đầy đủ nội dung bao gồm tiêu đề gói và nội dung gói.

Thiết lập một hệ thống giám sát mạng

Phần cứng chẩn đoán và xử lý sự cố mạng có thể nắm bắt dữ liệu đáng tin cậy và thường là hiệu quả nhất tại thu thập dữ liệu ở tốc độ đầy đủ của các phân đoạn mạng được giám sát. Tuy nhiên, các công cụ chẩn đoán và xử lý sự cố các mạng có một số nhược điểm mà làm cho họ không phù hợp để thực hiện giám sát mạng. Ví dụ, nó thiếu khả năng quản lý từ xa và không gian lưu trữ thích hợp, và nó thường có chi phí rất cao.

Các giải pháp phát hiện xâm nhập (IDS) đã giải quyết các vấn đề của quản lý từ xa và lưu trữ, và nó cũng có thể triển khai dễ dàng. Tuy nhiên, những nền tảng này có thể không đáng tin cậy khi thực hiện cả hai việc phát hiện xâm nhập và giám sát mạng cùng một lúc. Tất nhiên, nó là rất phổ biến cho một tổ chức sử dụng cảm biến IDS như là thiết bị giám sát mạng. Chỉ cần nhớ rằng một khi bạn hướng dẫn một cảm biến IDS để bắt đầu chụp toàn nội dung, tính hiệu quả của nó với vai trò là một cảm biến sẽ giảm.

Thiết lập một sniffer box để thực hiện giám sát mạng đòi hỏi một chút về kế hoạch và chuẩn bị. Khả năng của bạn để triển khai một sự giám sát có thể bị ảnh hưởng bởi kiến trúc mạng, băng thông đang được theo dõi, và thậm chí ảnh hưởng bên ngoài như chính trị của công ty hoặc một ngân sách hạn chế.

Việc tạo ra một hệ thống giám sát mạng lưới thành công bao gồm các bước sau:

- Xác định mục tiêu của bạn để thực hiện việc giám sát mạng.
- Đảm bảo rằng bạn có địa vị pháp lý thích hợp để thực hiện các hoạt động giám sát.
- Có được và thực hiện các phần cứng và phần mềm thích hợp.
- Đảm bảo sự an toàn của nền tảng này, cả về điện tử và vật lý.
- Đảm bảo các vị trí thích hợp của giám sát trên mạng.
- Đánh giá việc giám sát mạng của bạn.

Xác định mục đích

Bước đầu tiên để thực hiện giám sát mạng là phải biết lý do tại sao bạn đang làm nó ở nơi đầu tiên. Xác định các mục tiêu của giám sát mạng của bạn, vì chúng

sẽ ảnh hưởng đến phần cứng, phần mềm, và các bộ lọc bạn sử dụng để thu thập bằng chứng. Quyết định những gì bạn dự định thực hiện, chẳng hạn như:

- Xem traffic đến và đi từ một máy chủ cụ thể.
- Giám sát traffic đến và đi từ một mạng cụ thể.
- Giám sát hành động của một người cụ thể.
- Xác nhận nỗ lực xâm nhập.
- Tìm kiếm các dấu hiệu tấn công cụ thể.
- Tập trung vào việc sử dụng một giao thức cụ thể.

Khi bạn đã thiết lập mục tiêu của bạn cho mạng lưới giám sát, hãy đảm bảo rằng các chính sách bạn có ở nơi hỗ trợ các mục tiêu này. Tổ chức của bạn có thể áp dụng một chính sách mà trong đó, dưới những tình tiết giảm nhẹ, hoạt động email của một nhân viên được đặt dưới sự giám sát. Hãy chắc chắn rằng những chính sách này được vạch ra rõ ràng trước khi bắt đầu giám sát.

Lựa chọn phần cứng phù hợp

Bạn có thể mua một hệ thống thương mại hoặc xây dựng mạng lưới giám sát của riêng bạn. Vấn đề quan trọng là phải đảm bảo hệ thống của bạn có năng lực cần thiết để thực hiện chức năng giám sát của mình.

Tổ chức với ngân sách nhỏ sẽ cần phải dựa vào các giải pháp cây nhà lá vườn. Trong một số khía cạnh, các giải pháp được ưa chuộng hơn vì bạn có thể tùy chỉnh chúng cho phù hợp với nhu cầu cục bộ. Chọn một hệ thống mạnh mẽ, ổn định và dành nó để giám sát mạng.

Chọn phần mềm phù hợp

Có lẽ thách thức khó khăn nhất trong lắp ráp một mạng lưới giám sát được lựa chọn phần mềm cho nó. Công cụ giám sát có thể chiếm rất nhiều tiền, và bạn có thể cần các công cụ khác nhau để đáp ứng nhu cầu khác nhau. Bạn sẽ khám phá ra rằng các công cụ miễn phí chụp lưu lượng truy cập mạng nhiều cũng như, hoặc tốt hơn, các đối tác thương mại của họ. Tuy nhiên, các công cụ thương mại nói chung tốt hơn các tiện ích miễn phí khi nói đến việc phân tích và giải thích các lưu lượng được. Mỗi tiện ích dường như cung cấp một cái gì đó mà của người khác thì không, vì vậy bạn nên biết những gì bạn cần để có được ra khỏi phần

mềm giám sát mạng của bạn trước khi bạn có được nó. Dưới đây là một số yếu tố có thể ảnh hưởng đến các phần mềm mà bạn chọn:

- Những hệ điều hành nào bạn sẽ sử dụng?
- Bạn có muốn cho phép truy cập từ xa với màn hình của bạn hoặc truy cập vào quá trình giám sát của bạn chỉ ở console?
- Bạn có muốn thực hiện một silient sniffer trên mạng?
- Bạn có cần tính di động của các tập tin chụp?
- Các kỹ năng kỹ thuật của những người chịu trách nhiệm cho việc giám sát là gì?
- Bao nhiêu dữ liệu đi qua mạng?

Một số gói phần mềm sniffer thương mại phổ biến bao gồm Sniffer Network Analyzer cho Ethernet, Surveyor / Explorer, và Lan Analyzer. Lựa chọn một hệ điều hành phù hợp cũng quan trọng như việc lựa chọn các phần mềm sniffer thích hợp mà bạn quyết định sử dụng để giám sát mạng.

Hệ điều hành

Một số hệ điều hành tự nó phù hợp để thực hiện sniffing mạng. Rõ ràng, càng nhiều thời gian sẵn sàng của CPU và I / O cho các ứng dụng giám sát mạng, hệ thống sẽ hoạt động càng tốt hơn dưới một mạng tải nặng.

Khi bạn xây dựng nền tảng giám sát, hãy chắc chắn rằng bạn loại bỏ tất cả các ứng dụng và các quá trình đó là không cần thiết cho hoạt động của hệ điều hành, sniffer, và các chức năng quản trị. Điều này bao gồm việc loại bỏ bất kỳ môi trường người dùng đồ họa mà không cần thiết. Bạn không muốn bỏ lỡ các gói chỉ vì CPU bận rộn cố gắng để di chuyển một biểu tượng xung quanh màn hình!

Trong hàng chục hệ thống chúng ta đã làm chủ, một nền tảng Unix ổn định đã vượt xa các nền tảng khác. Đặc biệt, hệ điều hành FreeBSD đã cung cấp các môi trường chụp hiệu quả nhất, bởi vì các nhà phát triển đã sắp xếp hợp lý các chuyển động của khung mạng từ không gian bộ nhớ kernel (điểm chụp) tới không gian bộ nhớ sử dụng (các điểm lưu trữ).

Chúng tôi chọn FreeBSD như hệ điều hành cho các máy trạm giám sát vì nó cung cấp các tính năng sau:

- Hỗ trợ mạng TCP/IP mạnh mẽ
- Bảo mật, cho phép truy cập từ xa thông qua Secure Shell (SSH)
- Các cơ chế đơn giản để vô hiệu hóa các dịch vụ không cần thiết và thực hiện một bức tường lửa cục bộ
- Có khả năng chạy trên rất nhiều dạng phần cứng, với yêu cầu tối thiểu về bộ nhớ bộ xử lý
- Chi phí thấp - nó hoàn toàn miễn phí

Truy cập từ xa

Nếu bạn cần truy cập từ xa để giám sát, bạn có thể sử dụng kết nối mạng hoặc một modem. Một cách tiếp cận là để cài đặt một card mạng thứ hai, kết nối nó với một mạng riêng biệt hoặc mạng LAN ảo (VLAN), và sau đó cài đặt phần mềm lệnh cấp từ xa như OpenSSH.

Bạn nên ngăn chặn địa chỉ IP đến tới những trang web dưới sự kiểm soát của bạn.

Một lựa chọn khác là để truy cập vào hệ thống thông qua một modem cho kênh thông tin liên lạc "out-of-band", hoặc thông tin liên lạc mà không thể bị chặn một cách dễ dàng bởi một kẻ tấn công. Đảm bảo rằng các truy cập từ xa thông qua modem là an toàn bằng cách yêu cầu tối thiểu xác thực ID / mật khẩu của người dùng. Bạn cũng có thể cấu hình truy cập từ xa thông qua đường dây modem để nó chỉ chấp nhận các cuộc gọi đến từ số điện thoại cụ thể.

Silent Sniffers

Là khó khăn cho những kẻ xâm nhập để xóa bằng chứng khi họ không nhận thức được. Thực hiện một silent sniffer là cách hết sức rõ ràng nhất của việc ngăn chặn những kẻ xâm nhập khỏi việc khám phá hệ thống giám sát của bạn. Một silent sniffer là một hệ thống mà sẽ không đáp lại với bất kỳ gói dữ liệu gói nó nhận trực tiếp, broadcast hoặc multicast. Nhiều ứng dụng sniffer thương mại sẽ cấu hình adapter mạng cho bạn, đặt card mạng của bạn vào chế độ "tàng hình".

Các định dạng file dữ liệu

Khi chọn một công cụ để giám sát toàn bộ nội dung, sẽ là khôn ngoan để xem xét làm thế nào các thông tin thu trên hệ thống của bạn được lưu trữ. Hầu hết các ứng dụng thương mại có các định dạng tập tin độc quyền, mà có thể làm cho

việc chuẩn bị khó khăn trong trường hợp khi tổ chức thi hành pháp luật hay thương mại khác tham gia. Lựa chọn phần mềm tạo ra các tập tin theo một định dạng chuẩn mở sẽ giúp cho bạn (và những người khác) đỡ nhức đầu.

Dưới đây là một số ví dụ về sniffer, cả bản thương mại và bản miễn phí, mà sử dụng định dạng riêng cho các file chụp mà nó tạo ra.

- Lawrence Livermore National Labs (LLNL) libpcap-based sniffers (tcpdump, Ethereal, and Snort)
- Sun Solaris Snoop
- IBM AIX's iptrace
- HP-UX's nettl (Network Tracing and Logging Tool)
- Network Associates' Sniffer Pro
- AG Group's Etherpeek
- Novell's LANalyzer
- RADCOM's WAN/LAN Analyzer
- Cisco Secure Intrusion Detection System (CSIDS)

Triển khia giám sát mạng

Vị trí đặt giám sát mạng có thể là yếu tố quan trọng nhất trong việc thiết lập một hệ thống giám sát. Thiết bị và công nghệ mạng mới như mạng chuyển mạch, VLAN, và nhiều mạng tốc độ dữ liệu (10/100 Mb / giây Ethernet) đã tạo ra một số thách thức mới cho các nhà điều tra.

Các mục tiêu thông thường của mạng lưới giám sát là để nắm bắt tất cả các hoạt động liên quan đến một hệ thống mục tiêu cụ thể. Thiết bị chuyển mạch sẽ phân đoạn mạng bằng cách phát hiện sự hiện diện của máy trạm dựa trên địa chỉ MAC của họ. Sau khi switch xây dựng mỗi cổng với một địa chỉ MAC trong một quan hệ bảng, nó sẽ chuyển gói tin từ một cổng chỉ khi hệ thống nhận có trong bảng.

Đánh giá giám sát mạng

Khi thực hiện giám sát mạng, bạn có thể không chỉ đơn thuần là bắt đầu tcpdump và thực hiện từ giao diện điều khiển. Bạn sẽ muốn kiểm tra để chắc chắn rằng đĩa không đầy nhanh chóng, xác minh rằng các chương trình gói chụp được

thực hiện một cách thích hợp, và xem những gì sắp xếp của tải giám sát mạng được thực hiện.

Thực thi một Trap and trace

Như đã đề cập trong phần trước, để capture thông tin không nội dung từ một mạng, bạn có thể dùng *pen register* hoặc *trap-and-trace*. Trong mạng kết nối Internet, áp dụng một *trap-and-trace* trong mạng của bạn nghĩa là giám sát mào đầu (header) của gói tin IP và TCP, không giám sát bất cứ nội dung nào của gói tin.

Các giám sát Trap-và-trace là cực kỳ hữu ích trong trường hợp DoS, nơi mà họ có thể cung cấp bằng chứng khác so với chỉ lời khai bằng miệng rằng "router bị rơi sáu lần ngày hôm qua." Nếu mạng của bạn có một IDS, router, hoặc máy chủ web mà bí ẩn bị treo thường xuyên, thì một cái Trap-and-trace của tất cả các traffic mạng đến và đi từ các hệ thống nạn nhân không chỉ giúp xác định nguồn gốc của vấn đề, mà còn cung cấp manh mối tốt về việc sửa chữa kỹ thuật thích hợp. Nó cũng có thể được sử dụng như bằng chứng cho thấy các cuộc tấn công xảy ra.

Bạn có thể thực hiện một cái Trap-and-trace bằng cách sử dụng miễn phí, công cụ chuẩn như tcpdump, một tiêu chuẩn công nghiệp lâu năm. Ngoài ra còn có một tiện ích tcpdump cho các hệ thống Windows (Windows 95 và sau này) được gọi là WinDump, cực kỳ hữu ích khi thực hiện giám sát Trap-and-trace. WinDump là hoàn toàn tương thích với tcpdump và có thể được sử dụng để theo dõi và chẩn đoán lưu lượng mạng theo các quy tắc tương tự như tcpdump. WinDump sử dụng một thư viện libpcap-tương thích cho Windows gọi WinPcap. Như vậy, tcpdump và các tập tin chụp WinDump có định dạng nhị phân, vì vậy bạn có thể capture lưu lượng sử dụng tcpdump và xem bằng WinDump.

Thực thi Trap-and-Trace với WinDump

Như đã lưu ý ở trên, bạn có thể dụng WinDump, một công cj kiểm tcpdump cho hệ điều hành Widnows để thực thi trap-and-trace.

Tạo 1 fie đầu ra của Trap-and-Trace

Khi thực thi một trap-and-trace, nó sẽ đơn giản hơn để tạo 1 file đầu ra bằng tay so với việc xem dữ liệu trực tiếp từ console. Nếu không có một tập tin đầu ra, các thông tin bị mất những phút bạn chấm dứt quá trình tcpdump hoặc WinDump. Các dòng lệnh sau đây sẽ bắt đầu chụp các thông tin mào đầu (header) trên tất cả các traffic (không có bộ lọc) mà chạm đến các adapter mạng trên hộp sniffing:

```
[root@homer /root]# tcpdump > traptrace1
```

Nếu bạn đang ở trên một mạng bận rộn, một ý tưởng tốt là ngăn chặn dòng lệnh này một cách nhanh chóng, vì các tập tin traptrace1 có thể phát triển rất lớn trong một khoảng thời gian ngắn.

Để xem các tập tin chụp, bạn có thể sử dụng tiêu chuẩn Unix lệnh như `cat` and `more`, hoặc Linux's fancy `less` command. Ví dụ:

```
[root@homer /root]# cat traptrace1
```

Dùng TCPDump cho việc giám sát toàn dữ liệu

Sau khi bạn đã có hệ thống giám sát mạng của bạn thiết lập, bạn đã sẵn sàng để bắt đầu giám sát đầy đủ nội dung, thu thập các gói dữ liệu thô từ mạng. Các dòng lệnh sau đây bắt đầu bằng văn bản của các gói dữ liệu vào đĩa với tcpdump:

```
tcpdump -n -i dc0 -s 1514 -w

/var/log/tcpdump/emergency_capture.lpc &
```

- `-n` Không phân giải tên về đại chỉ IP hoặc port
- `-idc0` Lắng nghe trên cổng dc0. Cổng thiết bị không cần một địa chỉ IP để lưu các gói tin
- `-s1514` thiết lập "snap" với chiều dài là 1514 bytes.
- `-w/var/log/tcpdump` Ghi đầu ra của tcpdump vào 1 file trong thư mục /var/ tcpdump với tên emergency_capture.lpc.
- `&` Chuyển tiến trình này vào background.

Lọc dữ liệu toàn nội dung

Trong tình huống mà bạn đang thu thập quá nhiều lưu lượng truy cập cho hệ thống giám sát của bạn để xử lý, bạn sẽ cần phải lọc các dữ liệu đầy đủ nội dung. Cách đơn giản nhất để thực hiện lọc trong tcpdump dựa trên việc xây dựng bộ lọc Packet Berkeley. Các trang tcpdump dẫn cung cấp nhiều tùy chọn để chỉ sự chú ý của công cụ hướng các gói tin cụ thể.

Trong sự cố an ninh máy tính, chúng ta thường phụ thuộc vào việc xem traffic hoặc từ máy chủ hoặc tới máy chủ. Ví dụ, để ghi lại tất cả lưu lượng truy cập đến hoặc từ khối mạng 12.44.56.0/24, chúng ta sẽ sử dụng dòng lệnh sau đây:

```
tcpdump -n -i dc0 -s 1514 -w

/var/log/tcpdump/emergency_capture.lpc net 12.44.56 &
```

Dòng lệnh tiếp theo có thể được dùng để thu thấp tất cả traffic tới và từ một host cụ thể (IP address 172.16.1.7):

```
tcpdump -n -i dc0 -s 1514 -w
/var/log/tcpdump/emergency_capture.lpc host 172.16.1.7 &
```

Với yêu cầu thu thập tất cả traffic mạng từ khối mạng 12.44.56 và để thu thập tất cả gói tin tới và từ hệ thống có IP address là 172.16.1.7, bạn có thể sử dụng câu lệnh sau:

```
tcpdump -n -i dc0 -s 1514 -w
/var/log/tcpdump/emergency_capture.lpc net 12.44.56 or host
172.16.1.7 &
```

Khi bộ lọc của bạn bắt đầu trở nên phức tạp, bạn có thể đặt chúng trong một tập tin và tham khảo chúng từ dòng lệnh. Các tập tin sau đây có thể được sử dụng để thực hiện các ví dụ trước trong một định dạng gọn gàng đơn giản. Ví dụ, bạn có thể tạo một tập tin gọi là tcpdump.ips (tên tập tin này là tùy ý) với các nội dung:

```
net 12.44.56 or host 172.16.1.7
```

Bây giờ bạn có thể tham khảo tcpdump.ips từ dòng lệnh bằng cách sử dụng chuyển đổi -F:

```
tcpdump -n -i dc0 -s 1514 -w
/var/log/tcpdump/emergency_capture.lpc –F tcpdump.ips &
```

Duy trì các file dữ liệu toàn nội dung

Hai khía cạnh khác của việc thu thập đầy đủ các nội dung quan tâm dữ liệu bằng khen: filenaming và đảm bảo tính toàn vẹn file.

Đưa ra chụp tên tập yếu tố duy nhất giúp xác định nguồn gốc và mục đích của họ. Chúng tôi muốn bao gồm một dấu thời gian, tên máy và giao diện trong tên tập tin chụp. Để mở rộng bộ sưu tập ví dụ trước, chúng tôi có thể sử dụng sau đây:

```
tcpdump -n -i dc0 -s 1514 -w /var/log/tcpdump/`/bin/date "
+DMY_%d-%m-%Y_HMS_%H%M%S"`.`hostname`.dc0.lpc net 12.44.56 &
```

Câu lệnh đó sẽ thực thi 1 file với tên trong tham số, nếu bắt đầu vào February 10, 2003, lúc 15:18:50, trong 1 hệ thống tên là archangel, listening on interface dc0:

```
DMY_10_02_2003_HMS_151850.archangel.dc0.lpc
```

Bao gồm các `DMY` để nhắc nhở chúng ta rằng những ký tự tiếp theo là những ngày, tháng và năm. Các HMS xác định rằng giờ, phút, giây và làm theo. Tất nhiên, bạn có thể sử dụng một hệ thống khác nhau để phù hợp với sở thích cá nhân của bạn.

Ngoài việc sử dụng một quy ước đặt tên duy nhất, nó có tính pháp lý hữu ích để thực hiện hàm băm MD5 hoặc SHA của các tập tin dữ liệu đầy đủ nội dung. Cả Unix (md5 hoặc md5sum) và Windows (thông qua các ứng dụng của bên thứ ba, như md5sum.exe) cung cấp khả năng này. Đảm bảo tính toàn vẹn của bằng chứng là quan trọng với mạng lưới giao thông như đó là với thông tin thu thập được từ máy chủ điều tra pháp y.

Thu thập các file log mạng

Đừng bỏ qua tất cả các nguồn tiềm năng của các bằng chứng khi trả lời một sự cố! Hầu hết các mạng lưới giao thông để lại một dấu vết kiểm toán ở đâu đó dọc theo con đường nó đi. Dưới đây là một số ví dụ:

- Routers, firewalls, servers, IDS sensors, và các thiết bị mạng khác có thể duy trì các log mà ghi lại các sự kiện mạng
- Máy chủ DHCP lưu log truy cập mạng khi 1 PC yêu cầu cấp 1 IP

- Firewall hiện đại cho phép người quản trị một số lượng lớn chi tiết khi tạo các log giám sát
- Cảm biến IDS có thể bắt gặp một phần của một cuộc tấn công do một sự công nhận chữ ký hoặc bộ lọc phát hiện bất thường.
- Cảm biến Host-based có thể phát hiện sự thay đổi của một hệ thống thư viện hoặc bổ sung một tập tin trong một vị trí nhạy cảm.
- Hệ thống tập tin log ba vùng thời gian đi trên bộ điều khiển tên miền chính có thể hiển thị một xác thực thất bại trong một nỗ lực đăng nhập.

Xử lý sự cố truy cập trái phép

Định nghĩa

Một sự cố truy cập trái phép xảy ra khi một người cố truy cập vào tài nguyên mà người đó không được phép. Truy cập trái phép thường đạt được thông qua việc khai thác các hệ điều hành hoặc các lỗ hổng ứng dụng, việc mua lại tên người dùng và mật khẩu, các kỹ thuật xã hội. Những kẻ tấn công có thể có được quyền truy cập hạn chế thông qua một lỗ hổng và sử dụng truy cập đó để tấn công nhiều lỗ hổng hơn, cuối cùng đạt được cấp độ cao hơn của truy cập. Ví dụ về các sự cố truy cập trái phép bao gồm-

- Thực hiện một sự thỏa hiệp root từ xa của một máy chủ email
- Thay đổi giao diện một máy chủ Web
- Đoán hay phá mật khẩu
- Xem hoặc sao chép dữ liệu nhạy cảm, chẳng hạn như hồ sơ trả lương, thông tin y tế, và số thẻ tín dụng, mà không có phép
- Chạy một gói sniffer trên một máy trạm để nắm bắt các tên người dùng và mật khẩu
- Sử dụng một lỗi cho phép trên một máy chủ FTP nặc danh để phân phối phần mềm và các file âm nhạc vi phạm bản quyền
- Quay số tới một modem không có bảo đảm và được truy cập mạng nội bộ
- Trong vai trò là một giám đốc điều hành, kêu gọi sự giúp bàn, đặt lại mật khẩu email của giám đốc điều hành, và học hỏi mật khẩu mới
- Sử dụng một cài, máy trạm đăng nhập mà không có sự cho phép.

Chuẩn bị

Phần này cung cấp hướng dẫn về chuẩn bị để xử lý sự cố truy cập trái phép và về ngăn chặn sự cố truy cập trái phép.

Chuẩn bị xử lý sự cố

Một số hành động cần được thực hiện trong khi chuẩn bị để xử lý sự cố truy cập trái phép:

- Cấu hình dựa trên mạng và / hoặc phần mềm IDP dựa trên máy chủ (chẳng hạn như tập cờ vẹn và đăng nhập màn hình) để xác định và cảnh báo về những nỗ lực để đạt được quyền truy cập trái phép.
- Sử dụng máy chủ nhật ký tập trung thông tin quá thích hợp từ các host trên toàn tổ chức được lưu giữ tại một địa điểm duy nhất được bảo đảm.
- Thiết lập các thủ tục để được theo sau khi tất cả người dùng của một ứng dụng, hệ thống, miền tin cậy, hoặc tổ chức nên thay đổi mật khẩu của họ vì một thỏa hiệp mật khẩu. Các thủ tục cần tuân thủ các chính sách mật khẩu của tổ chức.
- Thảo luận về sự cố truy cập trái phép với quản trị hệ thống để họ hiểu rõ vai trò của họ trong quá trình xử lý sự cố.

Ngăn chặn sự cố

Số lượng các sự cố truy cập trái phép nên được giảm một cách hiệu quả. Sử dụng một chiến lược phòng thủ nhiều lớp mạnh mẽ, với nhiều lớp bảo mật giữa người sử dụng trái phép và các nguồn lực mà họ đang cố gắng để khai thác, là thực hành được đề nghị để giảm sự cố.

Phát hiện và phân tích

Bởi vì sự cố truy cập trái phép có thể xảy ra dưới nhiều hình thức, nó có thể được phát hiện thông qua hàng chục loại kinh nghiệm người đi trước và chỉ dẫn.

Sự cố truy cập trái phép khác nhau so với các loại sự cố trong đó nó có xu hướng xảy ra trong một vài bước. Thông thường, kẻ tấn công sẽ thực hiện nhiều hoạt động trinh sát để lập sơ đồ mạng; xác định các host; xác định những gì hệ điều hành, dịch vụ, và các ứng dụng mỗi máy chủ chạy; và tìm các lỗ hổng đó có thể khai thác từ xa. Trinh sát đã trở nên quá phổ biến mà các tổ chức thường bỏ

qua nó vì thời gian và nguồn lực hạn chế. Tuy nhiên, điều quan trọng cho các tổ chức để xem xét các hoạt động trinh sát, là tối thiểu nhất, để có được một cảm giác về những rủi ro mà họ đang phải đối mặt.

Sau khi các bước trinh sát đã được hoàn thành, những kẻ tấn công bắt đầu hành động để có được quyền truy cập trái phép vào hệ thống. Nhiều lỗ hổng cho phép quyền truy cập đạt được trong một bước duy nhất, trong khi các lỗ hổng khác chỉ cung cấp quyền truy cập người dùng cấp. Cuối cùng, hầu hết các kẻ tấn công đang tìm cách tiếp cận quản trị cấp cho hệ thống, do đó, họ thường tìm lỗ hổng đầu tiên có thể cấp quyền truy cập đặc quyền. Nếu một lỗ hổng như vậy không thể được tìm thấy hoặc khai thác thành công, kẻ tấn công có thể cố gắng để tìm và khai thác lỗ hổng có thể cung cấp cấp độ người dùng và sau đó thực hiện các cuộc tấn công thêm để nâng cao cấp độ truy cập. Bởi vì quá trình này có thể mất một số lượng đáng kể thời gian, các cuộc tấn công có thể được phát hiện tại một bước trung gian, khi một số truy cập đã được cấp trừ khi truy cập bổ sung đang được theo đuổi. Các đội phản ứng sự cố nên cố gắng để phát hiện, xác nhận, và ngăn chặn sự cố như vậy trước khi truy cập quản trị đầy đủ là đã đạt được. Nếu truy cập tăng tấn công cấp quyền quản trị, những kẻ tấn công có khả năng cài đặt rootkit và thiết lập các cửa hậu để họ có thể truy cập hệ thống từ xa với quyền quản trị trong tương lai.

Ngăn chặn, xoá, và phục hồi

Phần này cung cấp cho các khuyến nghị cụ thể để thực hiện ngăn chặn, và thu thập và xử lý các bằng chứng cho sự cố truy cập trái phép.

Lựa chọn một chiến lược ngăn chặn

Thời gian đáp ứng là rất quan trọng khi cố gắng để ngăn chặn một vụ việc truy cập trái phép. Phân tích sâu rộng có thể được yêu cầu để xác định chính xác những gì đã xảy ra; và trong trường hợp của một cuộc tấn công đang hoạt động, trạng thái của sự vật có thể được thay đổi nhanh chóng. Trong hầu hết các trường hợp, nó được khuyến khích để thực hiện một phân tích ban đầu của vụ việc, ưu tiên các vụ việc, thực hiện các biện pháp ngăn chặn ban đầu, và sau đó thực hiện phân tích sâu hơn để xác định nếu các biện pháp ngăn chặn là đủ.

Xử lý sự cố nên xem xét các giải pháp ôn hòa hơn là tập trung vào việc giảm thiểu các rủi ro đến mức thực tế, chứ không phải là đóng toàn bộ môi trường

trong nhiều ngày tại một thời điểm (trừ khi, tất nhiên, mức độ của các hoạt động độc hại là rất lớn mà shutdown hoàn toàn là xứng đáng). Một sự kết hợp thích hợp của các hành động sau đây phải có hiệu quả trong việc ngăn chặn ban đầu hoặc cuối cùng của một sự cố truy cập trái phép:

- Isolate the affected systems
- Disable the affected service
- Eliminate the attacker's route into the environment
- Disable user accounts that may have been used in the attack
- Enhance physical security measures

Thu thập bằng chứng và xử lý

Khi người xử lý nghi ngờ rằng việc truy cập trái phép đã đạt đến một hệ thống, họ nên thực hiện một sao lưu hình ảnh đầy đủ của hệ thống. Dữ liệu khác có liên quan, bao gồm cả máy chủ và ứng dụng các bản ghi, cảnh báo phát hiện xâm nhập, và các bản ghi tường lửa, có thể cung cấp bằng chứng về mối tương quan giữa các truy cập trái phép. Nếu vi phạm an ninh vật lý xảy ra trong vụ việc, bằng chứng bổ sung có thể có sẵn thông qua hệ thống các bản ghi bảo mật vật lý, băng camera an ninh, và nhân chứng. Sự cố truy cập trái phép có nhiều khả năng hơn so với hầu hết các sự cố khác dẫn đến truy tố, vì vậy điều quan trọng là phải tuân theo các bằng chứng thu thập được thành lập và xử lý các thủ tục và liên hệ với thực thi pháp luật nếu những giá trị tình hình tham gia của họ.

Xóa và Khôi phục

Kẻ tấn công thường xuyên cài đặt rootkit, trong đó sửa đổi hoặc thay thế những chương trình hệ thống và các file khác. Rootkit ẩn nhiều về những gì nó thực hiện, làm cho nó khó khăn để xác định những gì đã bị thay đổi. Vì vậy, nếu một kẻ tấn công dường như có được quyền root một hệ thống, người xử lý không thể tin tưởng vào hệ điều hành. Thông thường, các giải pháp tốt nhất là khôi phục hệ thống từ một bản sao lưu tốt được biết đến hoặc cài đặt lại hệ điều hành và các ứng dụng từ đầu, và sau đó làm an toàn hệ thống một cách đúng đắn. Thay đổi tất cả mật khẩu trên hệ thống, và có thể trên tất cả các hệ thống có mối quan hệ tin cậy với các hệ thống nạn nhân, cũng là rất khuyến khích.

Nếu kẻ tấn công chỉ đạt mức thấp hơn so với truy cập cấp quản trị, xóa và phục hồi các hành động cần phải dựa trên mức độ mà những kẻ tấn công đã đạt được quyền truy cập. Lỗ hổng đã được sử dụng để truy cập nên được giảm thiểu một cách thích hợp. Hành động bổ sung cần được thực hiện như xác định và chỉ rõ điểm yếu của hệ thống.

Danh sách kiểm tra cho Xử lý sự cố truy cập trái phép

Danh sách kiểm tra cung cấp các bước chủ yếu được thực hiện trong việc xử lý một sự cố truy cập trái phép.

Lưu ý rằng các trình tự chính xác của bước này có thể thay đổi dựa trên bản chất của sự cố cụ thể và trên các chiến lược được lựa chọn bởi tổ chức để đựng sự cố.

Table 4-4. Unauthorized Access Incident Handling Checklist

	Action	Completed
Detection and Analysis		
1.	Prioritize handling the incident based on its business impact	
1.1	Identify which resources have been affected and forecast which resources will be affected	
1.2	Estimate the current technical effect of the incident	
1.3	Find the appropriate cell(s) in the prioritization matrix, based on the technical effect and affected resources	
2.	Report the incident to the appropriate internal personnel and external organizations	
Containment, Eradication, and Recovery		
3.	Perform an initial containment of the incident	
4.	Acquire, preserve, secure, and document evidence	
5.	Confirm the containment of the incident	

5.1	Further analyze the incident and determine if containment was sufficient (including checking other systems for signs of intrusion)	
5.2	Implement additional containment measures if necessary	
6.	Eradicate the incident	
6.1	Identify and mitigate all vulnerabilities that were exploited	
6.2	Remove components of the incident from systems	
7.	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.	Create a follow-up report	
9.	Hold a lessons learned meeting	

Một số khuyến nghị

Các khuyến nghị chính được trình bày trong phần này để xử lý sự cố truy cập trái phép được tóm tắt dưới đây.

- **Configure intrusion detection software to alert on attempts to gain unauthorized access.** Mạng và phần mềm phát hiện xâm nhập dựa trên máy chủ (bao gồm toàn vẹn file phần mềm kiểm tra) là có giá trị cho việc phát hiện những nỗ lực để đạt được quyền truy cập trái phép. Mỗi loại phần

mềm có thể phát hiện sự cố mà các loại phần mềm có thể không, vì vậy việc sử dụng nhiều loại phần mềm bảo mật máy tính là rất khuyến khích.

- **Configure all hosts to use centralized logging.** Sự cố được dễ dàng hơn để phát hiện nếu dữ liệu từ tất cả các host trong toàn tổ chức được lưu giữ trong một bảo đảm vị trí tập trung.
- **Establish procedures for having all users change their passwords.** Một thỏa hiệp mật khẩu có thể buộc tổ chức này yêu cầu tất cả người dùng của một ứng dụng, hệ thống, hoặc tên miền hay niềm tin có lẽ là toàn bộ tổ chức để thay đổi mật khẩu của họ.
- **Configure the network perimeter to deny all incoming traffic that is not expressly permitted.** Bằng cách giới hạn các loại lưu lượng đến, kẻ tấn công sẽ có thể đạt được mục tiêu ít hơn và sẽ có thể đạt được mục tiêu bằng cách sử dụng giao thức chỉ định. Điều này sẽ giảm số lượng các sự cố truy cập trái phép.
- **Secure all remote access methods, including modems and VPNs.** Modem không có bảo đảm cung cấp các truy cập trái phép dễ dàng đạt được với các hệ thống nội bộ và mạng lưới. Khách hàng truy cập từ xa thường ngoài tầm kiểm soát của tổ chức, do đó cấp cho họ truy cập vào các nguồn tài nguyên làm tăng nguy cơ.
- **Put all publicly accessible services on secured DMZ network segments.** Điều này cho phép các tổ chức để cho phép máy chủ bên ngoài để khởi tạo kết nối đến máy chủ trên các phân đoạn DMZ chỉ, không để máy trên phân đoạn mạng nội bộ. Điều này sẽ giảm số lượng các sự cố truy cập trái phép.
- **Disable all unneeded services on hosts and separate critical services.** Mọi dịch vụ đang chạy trình bày một cơ hội tiềm năng cho sự thỏa hiệp. Tách các dịch vụ quan trọng là quan trọng bởi vì nếu một kẻ tấn công thỏa hiệp một máy chủ đang chạy một dịch vụ quan trọng, truy cập ngay lập tức nên chỉ đạt được với một dịch vụ.
- **Use host-based/personal firewall software to limit individual hosts' exposure to attacks.** Triển khai phần mềm dựa trên máy chủ hoặc tường lửa cá nhân với các host cá nhân và cấu hình nó để từ chối tất cả các hoạt động đó là không cho phép rõ ràng hơn nữa nên giảm khả năng sự cố truy cập trái phép.

- **Create and implement a password policy.** Các chính sách mật khẩu nên yêu cầu người sử dụng phức tạp, khó khăn để đoán mật khẩu và đảm bảo rằng các phương pháp xác thực là đủ mạnh để truy cập vào các nguồn tài nguyên quan trọng. Mật khẩu yếu và mặc định là có khả năng được đoán hoặc nứt, dẫn đến truy cập trái phép.
- **Provide change management information to the incident response team.** Chỉ định như tắt hệ thống, thay đổi cấu hình kiểm toán, và sửa đổi thực thi được có thể do quản trị hệ thống thông thường, chứ không phải là cuộc tấn công. Khi chỉ dẫn đó được phát hiện, nhóm nghiên cứu sẽ có thể sử dụng thông tin quản lý thay đổi để xác minh rằng các chỉ dẫn được gây ra bởi các hoạt động uỷ quyền.
- **Select containment strategies that balance mitigating risks and maintaining services.** Xử lý sự cố nên xem xét các giải pháp ngăn chặn vừa phải tập trung vào việc giảm thiểu các rủi ro nhiều như là thực tế trong khi duy trì các dịch vụ không bị ảnh hưởng.
- **Restore or reinstall systems that appear to have suffered a root compromise.** Các hiệu ứng của sự thỏa hiệp rễ thường rất khó để xác định hoàn toàn. Hệ thống này cần được khôi phục từ một bản sao lưu tốt được biết đến, hoặc hệ điều hành và các ứng dụng cần được cài đặt lại từ đầu. Hệ thống sau đó cần được bảo đảm đúng như vậy sự việc không thể tái phát.

Chương 5: Xử lý sự cố mã độc hại

Malware

Malware là một thuật ngữ được sử dụng thường xuyên nhưng thường xuyên áp dụng sai, vì vậy đầu tiên chúng ta hãy làm rõ ý nghĩa của nó. Thuật ngữ Malware là cách gọi ngắn gọn cho các malicious software - phần mềm độc hại, cái giả thích chính xác những gì loại phần mềm này được thiết kế để làm: để thực hiện các hành động độc hại và gây rối. Đơn giản, phần mềm độc hại là bất kỳ loại phần mềm thực hiện các hành động mà không cần sự đồng ý hay kiến thức của chủ sở hữu hệ thống và kết quả trong một hành động hoặc chuỗi hành động phá hoại.

Phần mềm độc hại và pháp luật

Hacker mũ trắng nên lưu tâm của các web của pháp luật có liên quan đến việc triển khai và sử dụng các phần mềm độc hại. Trong những năm qua, phần mềm độc hại đã gia tăng sự chú ý pháp lý như công nghệ đã tiến triển từ vô hại tới nhiều độc hại và mở rộng trong khả năng của mình. Việc tạo ra và sử dụng các phần mềm độc hại đã dẫn đến việc ban hành một số luật lệ rất nghiêm ngặt; nhiều quốc gia đã thông qua hoặc sửa đổi luật để ngăn chặn việc sử dụng các phần mềm độc hại.

Các loại phần mềm độc hại

Để hiểu được phần mềm độc hại là gì, chúng ta hãy nhìn vào các loại chủ yếu trước khi chúng tôi đào sâu hơn vào các cơ chế của mỗi loại:

- *Viruses* là hình thức nổi tiếng nhất từ trước đến nay của các phần mềm độc hại. Loại phần mềm độc hại được thiết kế để sao chép và đính kèm chính nó để các tập tin thường trú trên hệ thống. Thông thường, virus yêu cầu một số loại hành động của người để bắt đầu các hoạt động truyền nhiễm.
- *Worms* là một hình thức kế nhiệm cho các loại virus. *Worms* đã được hình thành kể từ cuối những năm 1980. *Worms* đầu tiên là nguyên thủy tiêu chuẩn hiện nay, nhưng vẫn thấy một số đặc tính mà tồn tại đến ngày hôm nay: khả năng tái tạo của chính nó rất nhanh chóng. Worms đã nổi lên trong

những thập kỷ qua đã được chịu trách nhiệm cho một số các tấn công từ chối dịch vụ tấn công nghiêm trọng nhất được biết đến.

- *Trojan horse* là một loại đặc biệt của phần mềm độc hại dựa phần lớn trên kỹ thuật social engineering để bắt đầu lây nhiễm cho một hệ thống và gây ra thiệt hại. Tương tự như một vi-rút trong nhiều khía cạnh, phần mềm độc hại này dựa vào người dùng bằng cách nào đó dụ dỗ vào tung ra các chương trình bị nhiễm bệnh hoặc gói tin, rồi lần lượt bắt đầu các Trojan.
- *Rootkit* là một hình thức hiện đại của phần mềm độc hại mà có thể ẩn trong các thành phần cốt lõi của hệ thống và ở lại không bị phát hiện bởi máy quét hiện đại. Điều gì làm cho rootkit nguy hại nhất là họ có thể cực kỳ khó khăn để phát hiện và thậm chí khó khăn hơn để loại bỏ.
- *Spyware* là phần mềm độc hại được thiết kế để thu thập thông tin về một hệ thống hoặc các hoạt động của người dùng một cách lén lút. Spyware đến trong nhiều hình thức; trong đó phổ biến nhất là keylogger.
- *Adware* là phần mềm độc hại mà có thể thay thế các trang chủ trong trình duyệt, đặt quảng cáo pop-up trên máy tính để bàn của người dùng, hoặc cài đặt các mục trên hệ thống của nạn nhân được thiết kế để quảng cáo sản phẩm hoặc dịch vụ..

Xử lý sự cố Mã độc

Định nghĩa sự cố và ví dụ

Mã độc dùng để chỉ một chương trình được bí mật đưa vào một chương trình khác với ý định phá hủy dữ liệu, chạy các chương trình phá hoại hay xâm nhập, hoặc nếu không thỏa hiệp về bảo mật hoặc tính bí mật, tính toàn vẹn và tính sẵn sàng của dữ liệu, các ứng dụng, hoặc hệ điều hành của nạn nhân. Nói chung, mã độc hại được thiết kế để thực hiện các chức năng này bất chính mà không cần sử dụng kiến thức của hệ thống. Khi tham chiếu trong NIST SP 800-83, Hướng dẫn Malware và phòng chống sự cố và xử lý, có rất nhiều loại mã độc hại, bao gồm virus, worms, trojan, mã độc hại di động, và tấn công hỗn hợp. Malware cũng bao gồm các công cụ tấn công như backdoor, rootkit, và keystroke logger, và theo dõi các tập tin cookie được sử dụng như phần mềm gián điệp.

Sự chuẩn bị

Phần này cung cấp hướng dẫn về chuẩn bị để xử lý sự cố mã độc hại và ngăn chặn sự cố về mã độc.

Chuẩn bị xử lý sự cố

Một số hành động cần được thực hiện để chuẩn bị cho việc xử lý sự cố mã độc hại:

- **Làm cho người dùng nhận thức của vấn đề về mã độc hại**. Thông tin này nên bao gồm một đánh giá cơ bản của phương pháp mà mã độc sử dụng để tuyên truyền và các triệu chứng của nhiễm trùng. Tổ chức các buổi đào tạo người dùng thường xuyên giúp đảm bảo rằng người dùng nhận thức được những rủi ro mà mã độc gây ra. Người dùng cũng sẽ nhận được lời khuyên về những gì họ nên làm gì nếu xảy ra lây nhiễm (ví dụ, ngắt kết nối máy trạm từ mạng, gọi bàn trợ giúp) bởi vì xử lý không đúng của một lây nhiễm có thể làm cho một sự cố nhỏ tồi tệ hơn nhiều.
- **Đọc các bản tin nhà cung cấp chương trình chống vi-rút**. Người dùng có thể đăng ký danh sách gửi thư từ nhà cung cấp chống vi-rút cung cấp thông tin kịp thời về mã độc hại mối đe dọa mới.
- **Triển khai hệ thống phát hiện xâm nhập dựa trên máy chủ đối với máy chủ quan trọng**. Dựa trên phần mềm máy chủ lưu trữ IDPS có thể phát hiện các dấu hiệucủa sự cố mã độc hại, chẳng hạn như thay đổi cấu hình và sửa đổi thực thi hệ thống. Người kiểm tra tính toàn vẹn của tập tin là hữu ích trong việc xác địnhcác thành phần bị ảnh hưởng của một hệ thống.
- **Thu thập tài nguyên phân tích sự cố phần mềm độc hại.** Các tổ chức nên có các nguồn lực phân tích thích hợp có sẵn trước khi xảy ra sự cố. Danh sách Port, tài liệu hệ điều hành, tài liệu ứng dụng, sơ đồ mạng, danh mục tài sản quan trọng, và đường cơ sở của mạng dự kiến, hệ thống, và các hoạt động ứng dụng tất cả nên có sẵn để hỗ trợ trong việc xác định và xác minh sự cố.
- **Có được phần mềm giảm nhẹ sự cố phần mềm độc hại.** Để hỗ trợ việc phục hồi, tổ chức phải đảm bảo các phần mềm giảm nhẹ thích hợp

có sẵn. Tổ chức cần phải có hệ điều hành đĩa khởi động và đĩa CD, các bản vá lỗi bảo mật từ các hệ điều hành và các nhà cung cấp ứng dụng, phần mềm và hình ảnh đĩa và sao lưu sạch có sẵn.

Ngăn chặn sự cố

Các lời khuyên về phòng ngừa sự cố mã độc hại:

- Sử dụng phần mềm antivirus
- Ngăn chặn cài đặt phần mềm gián điệp
- Khóa file bị nghi ngờ
- Lọc thư rác
- Giới hạn việc sử dụng các chương trình không thiết yếu với khả năng chuyển tập tin
- Giáo dục người dùng về xử lý an toàn của tập tin đính kèm Email
- Loại bỏ cửa sổ đang mở chia sẻ
- Sử dụng Web bảo mật trình duyệt để hạn chế mã nguồn di động
- Ngăn chặn mở chuyển tiếp thư điện tử
- Cấu hình Email client để hành động an toàn hơn

Phát hiện và phân tích

Tổ chức cần phải phấn đấu để phát hiện và xác nhận sự cố phần mềm độc hại nhanh chóng, vì lây nhiễm có thể lây lan qua các tổ chức trong một vài phút. Phát hiện sớm có thể giúp tổ chức giảm thiểu số lượng các hệ thống bị nhiễm, nên giảm bớt tầm quan trọng của các nỗ lực phục hồi và mức độ tổn hại tổ chức duy trì. Mặc dù sự cố lớn có thể tấn công một tổ chức một cách nhanh chóng mà không có thời gian cho bất cứ ai phản ứng, hầu hết các sự cố xảy ra chậm hơn.

Ưu tiên hóa sự cố mã độc đúng là quan trọng vì xu hướng của họ để lây lan sang các hệ thống khác. Trong hầu hết các trường hợp, một phân tích cơ bản của vụ việc nên xác định mã độc hại đã được sử dụng.

Sau đó nó tương đối dễ dàng để xác định các tác động có thể xảy ra của sự cố. Người xử lý sự cố có thể chưa được nhận thức của tất cả các hệ thống đã bị lây nhiễm trong sự cố; nhưng trong nhiều trường hợp, nó nên được rõ ràng cho dù vụ việc liên quan đến chỉ một vài hệ thống hoặc hàng ngàn máy chủ và máy trạm trong toàn tổ chức. Tổ chức phải thiết lập một tập hợp các tiêu chuẩn mà xác định

mức độ thích hợp của phản ứng cho các tình huống liên quan đến phần mềm độc hại khác nhau. Các tiêu chí cần cân nhắc kết hợp như sau:

- Làm thế nào các phần mềm độc hại vào môi trường và những cơ chế truyền tải nó sử dụng
- Những loại phần mềm độc hại được (ví dụ, virus, worm, Trojan horse)
- Những loại công cụ tấn công được đặt vào hệ thống bằng các phần mềm độc hại
- Những gì các mạng và hệ thống các phần mềm độc hại đang ảnh hưởng và làm thế nào nó ảnh hưởng đến họ
- Làm thế nào tác động của vụ việc có thể sẽ tăng trong những phút, giờ, và ngày sau nếu sự việc không được chứa.

Ngăn chặn, xoá, và phục hồi

Ngoài những hướng dẫn tổng quát, phần này cung cấp cho các khuyến nghị cụ thể để thực hiện ngăn chặn và để thu thập và xử lý các bằng chứng cho sự cố mã độc.

Lựa chọn một chiến lược ngăn chặn

Bởi vì mã độc hoạt động lén lút và có thể lan truyền đến hệ thống khác nhanh chóng, ngăn chặn sớm một sự cố mã độc hại là cần thiết để ngăn chặn nó lây lan và gây hại. Nếu hệ thống bị nhiễm là không quan trọng, ngắt kết nối từ mạng ngay lập tức được khuyến khích. Nếu hệ thống thực hiện các chức năng quan trọng, nó nên lưu trên mạng khi các thiệt hại cho các tổ chức từ các dịch vụ là không sẵn sàng là lớn hơn những rủi ro an ninh đặt ra do không ngay lập tức ngắt kết nối hệ thống. Hành động khác có thể cần phải được thực hiện khi có một sự cố mã độc hại như sau:

- Xác định và Cô lập máy chủ khác bị nhiễm
- Gửi mã độc hại chưa biết đến nhà cung cấp antivurs
- Cấu hình email server và email client để chặn email
- Ngăn chặn máy chủ cụ thể
- Tắt máy chủ thư điện tử
- Cô lập mạng từ Internet
- Thúc đẩy người dùng tham gia

- Vô hiệu hóa dịch vụ
- Vô hiệu hoá kết nối

Thu thập bằng chứng và xử lý

Mặc dù chắc chắn là có thể để thu thập bằng chứng về sự cố mã độc hại, nó thường là vô ích vì mã độc hại hoặc là truyền tự động hoặc là vô tình lây truyền qua người sử dụng bị nhiễm bệnh. Do đó, rất khó khăn và tốn nhiều thời gian để xác định nguồn gốc của mã độc. Có ba loại có thể có của các kỹ thuật nhận dạng vật chủ bị nhiễm:

- Xác định pháp y
- Chủ động nhận dạng
- Xác định thủ công

Xóa và phục hồi

Phần mềm antivirus và antispyware hiệu quả xác định và loại bỏ nhiễm trùng mã độc hại; tuy nhiên, một số tập tin bị nhiễm không thể được diệt. (Tập tin có thể được xóa và thay thế bằng bản sao dự phòng sạch; trong trường hợp của một ứng dụng, ứng dụng bị ảnh hưởng có thể được cài đặt lại.) Nếu mã độc hại cung cấp cho kẻ tấn công quyền truy cập root, nó có thể là không khả thi để xác định những hành động gì khác mà kẻ tấn công có thể đã thực hiện. Trong trường hợp này, hệ thống nên được khôi phục từ bản sao lưu trước đó, hoặc các bản backup sạch hoặc xây dựng lại từ đầu. Khi mức độ thiệt hại hoặc các truy cập trái phép vào một hệ thống là không rõ ràng, tổ chức nên cân nhắc việc xây dựng lại hệ thống. Hệ thống sau đó nên được bảo đảm để rằng nó sẽ không được dễ bị một nhiễm từ mã độc hại tương tự

Danh sách kiểm tra để xử lý sự cố mã độc

Danh sách kiểm tra cung cấp các bước chính được thực hiện trong việc xử lý sự cố mã độc hại.

Ví dụ về bảng danh sách kiểm tra cho xử lý sự cố mã độc

	Hành động	Hoàn thành

Detection and Analysis		
1.	Ưu tiên xử lý sự kiện dựa trên tác động kinh doanh của nó	
1.1	Xác định các nguồn tài nguyên đã bị ảnh hưởng và dự báo tài nguyên nào sẽ bị ảnh hưởng	
1.2	Ước tính hiệu quả kỹ thuật hiện tại và tiềm năng của sự kiện	
1.3	Tìm các tế bào thích hợp (s) trong ma trận ưu tiên, dựa trên hiệu ứng kỹ thuật và nguồn lực bị ảnh hưởng	
2.	Báo cáo sự việc cho các nhân viên nội bộ thích hợp và tổ chức bên ngoài	
Ngăn chặn, xoá, và phục hồi		
3.	Chứa các sự cố	
3.1	Xác định hệ thống bị nhiễm bệnh	
3.2	Ngắt kết nối hệ thống bị nhiễm bệnh từ mạng	
3.3	Giảm thiểu các lỗ hổng bị khai thác bởi mã độc hại	
3.4	Nếu cần thiết, ngăn chặn các cơ chế truyền dẫn cho mã độc hại	
4.	Xóa bỏ các sự cố	
4.1	Khử trùng, cách ly, xóa và thay thế các tập tin bị nhiễm bệnh	
4.2	Giảm thiểu các lỗ hổng khai thác cho máy khác trong tổ chức	
5.	Phục hồi từ sự kiện	
5.1	Xác nhận rằng các hệ thống bị ảnh hưởng đang hoạt động bình thường	

5.2	Nếu cần thiết, thực hiện giám sát bổ sung để tìm các hoạt động có liên quan trong tương lai	
Sau khi gặp sự cố hoạt động		
6.	Tạo một báo cáo theo dõi	
7.	Tổ chức một cuộc họp bài học kinh nghiệm	

Khuyến nghị

Các khuyến nghị chính trình bày trong phần này để xử lý sự cố mã độc hại được tóm tắt dưới đây.

- **Làm cho người dùng biết về các vấn đề mã độc hại**. Người dùng nên quen thuộc với các phương pháp mã độc sử dụng để tuyên truyền và các triệu chứng của nhiễm trùng. Tổ chức các buổi giáo dục người dùng thường xuyên giúp đảm bảo rằng người dùng nhận thức được những rủi ro mà mã độc gây ra. Dạy người sử dụng như thế nào để xử lý một cách an toàn file đính kèm email nên giảm số bệnh khác cũng xảy ra.
- **Đọc bản tin antivirus**. Bản tin về các mối đe dọa mã độc mới cung cấp thông tin kịp thời để xử lý sự cố.
- **Triển khai hệ thống phát hiện và phòng chống xâm nhập host-based, trong đó có kiểm tra tính toàn vẹn file, với các host quan trọng**. Phần mềm host-based IDPS phần mềm, đặc biệt là kiểm tra tính toàn vẹn tệp, có thể phát hiện các dấu hiệu của sự cố mã độc hại, chẳng hạn như thay đổi cấu hình và sửa đổi để thực thi.
- **Sử dụng phần mềm chống vi-rút, và giữ cho nó cập nhật mới nhấ**t. Phần mềm chống vi-rút nên được bố trí đến tất cả máy chủ và tất cả các ứng dụng có thể bị dùng để chuyển mã độc hại. Phần mềm nên được cấu hình để phát hiện và khử hoặc cách ly mã độc hại nhiễm trùng. Phần mềm chống vi-rút tất cả nên được giữ hiện tại với chữ ký virus mới nhất do đó, các mối đe dọa mới nhất có thể được phát hiện.
- **Cấu hình phần mềm để chặn các tập tin đáng ngờ**. Các file có nhiều khả năng là độc hại nên bị chặn từ môi trường, chẳng hạn như những

người có phần mở rộng tập tin mà thường được kết hợp với mã độc hại, cũng như các tập tin đáng ngờ với sự kết hợp của các phần mở rộng tập tin

- **Loại bỏ mở chia sẻ trên Windows**. Nhiều Worms lây lan qua các chia sẻ không có bảo đảm trên máy chủ chạy Windows. Một máy nhiễm duy nhất có thể nhanh chóng lây lan đến hàng trăm hoặc hàng ngàn các máy chủ thông qua chia sẻ không có bảo đảm.

- Loại bỏ mã sự cố độc hại một cách nhanh chóng nhất có thể. Bởi vì mã độc hại hoạt động bí mật và có thể truyền cho các hệ thống khác nhanh chóng, ngăn chặn đầu của một sự cố mã độc hại là cần thiết để ngăn chặn nó từ lây lan và gây thêm thiệt hại. Hệ thống bị nhiễm nên được ngắt khỏi mạng ngay lập tức. Tổ chức có thể cần phải ngăn chặn mã độc hại ở mức độ hệ phục vụ thư điện tử, hoặc thậm chí tạm thời đình chỉ dịch vụ email để đạt được kiểm soát nghiêm trọng emailborne mã độc hại sự cố

Chương 6: Xử lý mối đe dọa nội bộ

Chương này tập trung vào việc bảo vệ mạng của bạn từ bên trong, với giả định rằng tất cả các nỗ lực an ninh bên ngoài của bạn là vô ích nếu an ninh bên trong là một người bị ngã. Thứ hai, bởi vì "việc bên trong" hiếm khi khá hay chào đón, điều này chi tiết chương một số thực tiễn mà tránh trong các trường hợp tốt nhất, và phát hiện và trừng phạt trong trường hợp tồi tệ nhất, một kẻ xâm nhập ở giữa các ngươi.

An ninh nội bộ: Bước Red-Headed con

Trong thực tế, mặc dù theo khảo sát về bảo mật và tội phạm máy tính mới đây nhất của Viện bảo mật máy tính nói rằng 90% số người được hỏi phát hiện vi phạm an ninh, báo cáo đi vào để nói rằng chỉ có 40% số người được hỏi phát hiện hành vi vi phạm từ bên ngoài.

Các cuộc điều tra tiếp tục khẳng định rằng 78% số người được hỏi phát hiện truy cập trái phép của người trong cuộc. Rõ ràng, an ninh nội bộ là một vấn đề rất lớn. Các ICSA (Hiệp hội An ninh máy tính quốc tế) đồng ý, tin rằng người trong cuộc gây ra 80% các vấn đề an ninh.

Rủi ro nội bộ: Các loại tác hại và Vectors

Một số trong những loại phổ biến của tác hại mà bạn sẽ muốn xem xét là:

- Thỏa hiệp máy chủ
- Mạng thỏa hiệp cơ sở hạ tầng
- Application cấp thỏa hiệp
- Workstation thỏa hiệp (Trojan)
- mất hoặc bị đánh cắp dữ liệu độc quyền
- Việc truyền dữ liệu không phù hợp hoặc có hại cho các đối tác kinh doanh
- tấn công từ chối dịch vụ

Người lao động Có ý tốt / không có ý thức

Bất kỳ nhân viên của bạn có thể rơi vào thể loại này dưới ảnh hưởng của các chiến lược của hacker social engineering. Social engineering là hành vi sử dụng các kỹ năng liên cá nhân để có làm mọi người đưa ra những thông tin. Kỹ thuật này không được sử dụng rộng rãi, nhưng là có, một số hacker có kỹ năng social engineering.

Phương pháp của họ có thể khá khéo léo. Có lẽ một hacker chú ý đến thảo luận về sở thích trên một số diễn đàn của một nhân viên cấp thấp – đến cấp trung được đưa lên từ một ISP thay vì dải IP thông thường của công ty bạn. Các hacker sau đó có thể gọi là một quản trị viên CNTT trong công ty giả danh là nhân viên đó, và giải thích rằng ông đang telecommuting ngày hôm nay, máy của mình bị rơi và anh ta phải cài đặt lại, và ông cần phải biết thông tin cài đặt VPN (Virtual Private Network). Giả sử một tổ chức lớn và một admin không biết rõ giọng nói đó của nhân viên, cô chỉ có thể cung cấp các thông tin ra.

Nhân viên Scofflaw

Scofflaw employees là các nhân viên muốn bỏ qua các biện pháp bảo mật thông thường của bạn để thuận lợi riêng cho họ-có thể cũng là một vấn đề rất lớn.

Các ví dụ điển hình của một scofflaw employee là một trong những người bỏ qua chính sách, bỏ qua cơ chế truy cập từ xa của tổ chức, và quyết định cài đặt một modem và PCAnywhere trên PC của cô ta - nhiều lần mà không có một mật khẩu hợp lý tốt. Tất cả là một bất ngờ, có một cánh cửa mở từ bên ngoài vào mạng nội bộ của bạn - một điều không tốt.

Nhân viên IT

Tất nhiên, chỉ vì "tất cả mọi người" bây giờ là một vấn đề tiềm năng không có nghĩa là nhân viên IT bất mãn và lập trình viên không có thiết lập đặc biệt của riêng họ quan tâm. Nhiều đặc quyền tiềm năng có nghĩa là vấn đề tiềm năng hơn.

Chính sách giảm thiểu rủi ro

Bạn sẽ muốn thiết lập chính sách bằng văn bản, rõ ràng trong hợp tác với đội ngũ quản lý của tổ chức. Sự hợp tác này không thể được nhấn mạnh đủ thì

một chính sách không có hiệu lực cũng có thể không bao giờ được viết. Bạn sẽ muốn

- Thiết lập bảo mật vật lý tốt cho tất cả các cơ sở hạ tầng không có vấn đề như thế nào không đáng kể một phần của cơ sở hạ tầng có vẻ.
- Nhận quản lý để xây dựng một số mức độ quan tâm về an ninh mạng vào quá trình tuyển dụng.
- Rõ ràng cấm bỏ qua trạm kiểm soát an ninh (như tường lửa, máy chủ truy cập từ xa, vv) trong AUP của bạn.
- Thiết lập các chính sách quản lý máy tính để bàn có liên quan đến virus / bảo vệ và mức độ của các máy trạm lockdown Trojan.
- Khuyến khích các đội nhỏ của các quản trị viên để cộng tác. Nếu có nhiều hơn một người quản trị xem các chuồng gà, nó ít hấp dẫn đối với những con cáo.
- hệ thống phát hiện xâm nhập sử dụng (IDS), được cẩn thận để sử dụng những người có thể xử lý các mạng nội bộ băng thông cao.
- Kiểm toán hệ thống và thủ tục của bạn theo định kỳ.
- Duy trì mức hiện tại của hệ điều hành và các ứng dụng của các nhà cung cấp thường vá script kiddie khai thác khá nhanh chóng.

Bảo mật vật lý

Dưới đây là một số "nên" và "không nên làm" làm cho công việc của bạn dễ dàng hơn một chút, cuộc sống của một kẻ xâm nhập một chút khó khăn hơn, và dữ liệu của bạn an toàn hơn một chút:

- NÊN khóa bất cứ tủ dây và giữ chúng bị khóa.
- NÊN sử dụng switch thay cho hub, đặc biệt là cho các phân đoạn mạng LAN có người dùng quản trị trên chúng. (Họ vẫn phải bảo mật vật lý để đảm bảo ai đó không thể truy cập vào switch và sniff gói tin thông quan cơ chế port mirroring.) Chênh lệch giá giữa hub và switch đã giảm đáng kể trong những năm gần đây.
- NÊN thay đổi hoặc mật mã cửa, và mật khẩu cho bất kỳ tài khoản chia sẻ ngay lập tức khi nhân viên rời.
- NÊN xóa ổ đĩa cứng, flash, và tương tự, khi bạn đưa chúng ra khỏi dịch vụ.

- NÊN ghi dữ liệu vô nghĩa lên phương tiện truyền thông từ tính khi bạn đang xóa nó. Thả một bảng phân vùng là không đủ tốt. (mặc dầu vậy, Degaussing là tốt)
- NÊN sử dụng máy hủy tài liệu. Đừng cười. Dumpster là phổ biến hơn bạn nghĩ.
- NÊN khóa tủ máy chủ của bạn khi bạn không sử dụng chúng.
- NÊN hạn chế hoặc cấm sử dụng các modem trên máy tính để bàn; họ là số một trong những phương pháp bỏ qua trạm kiểm soát an ninh của tổ chức bạn.
- NÊN đảm bảo rằng bất kỳ "con đường" máy tính xách tay hoặc PDA có phần mềm bảo vệ dữ liệu thích hợp và phần cứng được cài đặt trước khi triển khai.
- NÊN xem xét liệu người dùng có hay không truy cập vào các đĩa mềm hoặc phương tiện di động khác có ý nghĩa đối với môi trường của bạn; chúng tạo thành một đường vòng có thể bỏ qua các trạm kiểm soát an ninh của bạn.
- NÊN xem xét việc sử dụng thẻ thông minh / thiết bị bảo mật token dựa chứ không phải là mật khẩu cho người dùng quản trị hoặc các hệ thống nhạy cảm. Nhiều hệ điều hành bây giờ hỗ trợ xác thực token dựa thêm vào mật khẩu.
- NÊN nhớ rằng PBX điện thoại của bạn cũng phải được bảo đảm.
- KHÔNG gửi off-trang web sao lưu đến các địa điểm không có bảo đảm.
- KHÔNG đưa chìa khóa để các nhà cung cấp. Hãy để họ ở để làm công việc của họ, và sau đó một cách lịch sự vẫy tay bye-bye khi họ rời khỏi.
- KHÔNG cho phép bất cứ ai khác ngoài nhân viên chìa khóa truy cập đặc biệt để các trung tâm dữ liệu.
- KHÔNG chia sẻ closets dây với thiết bị ngoại vi sử dụng theo định hướng như máy in.
- KHÔNG đặt máy chủ vào các khu vực không có bảo đảm.
- KHÔNG để khóa máy chủ gắn vào mặt sau của một máy chủ. Tin hay không, người khác sẽ nghĩ về điều này, quá.
- KHÔNG để làm sạch dân hoặc các khu vực khác đảm bảo dịch vụ không tin cậy người-thành mà không có một hộ tống.

- KHÔNG lưu trữ bất kỳ dữ liệu nhạy cảm trên ổ đĩa cứng của người dùng, nếu bạn phải, suy nghĩ về sản phẩm mã hóa ổ đĩa cứng.
- KHÔNG thảo luận về mật khẩu hoặc các thông tin nhạy cảm khác trên các kênh không có bảo đảm như điện thoại di động, điện thoại không dây, radio 800MHz, hay tin nhắn tức thời.
- KHÔNG đặt game, bàn phím, hay các máy trạm hành chính gần cửa sổ.

Quy trình tuyển dụng

Có những điều bạn có thể làm để giảm thiểu rủi ro của bạn trong quá trình tuyển dụng. Bắt đầu bằng cách làm một bài kiểm tra nền tảng "mẫn cán" – đặc biệt cho những nhân viên sẽ liên quan tới bất cứ cấp độ IT nào. Làm bài tập ở nhà của bạn và sử dụng một cơ quan có uy tín để làm kiểm tra nền tảng cùng với mọi thứ khác trong computing, “rác vào, rác thải ra”. Nếu bạn đang sử dụng một kiểm tra nhân sự nội bộ hoặc một số kiểm tra khác mà bạn không được lập hoá đơn, giao tiếp là chìa khóa. Đừng cho rằng sự im lặng từ bài kiểm tra nền tảng của bạn có nghĩa là "Tất cả mọi thứ là OK"

Sau khi bạn đã làm việc với quản lý để thành lập một Chính sách sử dụng chấp nhận được, bước tiếp theo của bạn là làm việc với bộ phận nhân sự để tích hợp nó như một phần của quá trình làm việc cho bất kỳ nhân viên.

Thiết lập Desktop Lockdown

Lockdown, trong bối cảnh quản lý máy tính để bàn, có nghĩa là bạn đã quản lý để áp dụng các dây đai vào người dùng của bạn theo cách mà họ không thể làm tổn thương mình hay mạng của bạn. Trong trường hợp tốt nhất, điều này được thực hiện trong một cách mà người dùng không cảm thấy bó buộc.

Cần lưu ý rằng quản lý desktop đó - bất kỳ quản lý desktopp nào - mà cư trú trên một máy trạm địa phương có thể được bỏ qua bởi một người dùng thông minh, trừ khi có bảo mật vật lý nghiêm túc tại chỗ (không có đĩa mềm, một "unpickable" trường hợp khóa, và vv) . Điều này, tất nhiên, là loại bảo mật mà bạn phải có nếu bạn có thiết bị đầu cuối thông tin công cộng, ki-ốt, và như vậy. Đó là điểm mà bất kỳ máy trạm mà không có bảo mật vật lý có thể được khởi động từ phương tiện truyền thông thay thế, và sau đó hệ điều hành cục bộ có thể được sửa đổi để cho người sử dụng độc hại.

Hạn chế Content

Nó được sử dụng để các nhà quản lý IT chỉ lo lắng về những gì người dùng đã có thể tải về; nghĩa là, những người thân lo ngại về tình trạng lạm dụng lao động của Internet. Vào thời điểm đó, không có công nghệ để kiểm tra những nội dung tải về thực tế là gì – nên các nhà quản lý bằng lòng với bản thân với chặn các trang web dựa trên nơi mà người dùng cố gắng để lướt. Một số nhà sản xuất phần mềm cũng đã trở thành tổ chức dịch vụ mà duy trì một danh sách các URL theo một số loại: định hướng người lớn, hài kịch, mua sắm, tin tức, và tương tự. Là nhà quản lý, bạn sẽ ngăn chặn nhiều loại khác nhau với một thiết bị ngoại vi mà có quyền truy cập vào danh sách này.

Chiến lược này, tuy nhiên, đã không được hoàn thành. Các trang web bị phản đối xuất hiện trở lại ngay trong đêm, và danh sách đã không luôn luôn phản ánh hiện thực. Và, lọc URL outbound không làm gì để chống lại các trang có nội dung đáng ngờ rời khỏi tổ chức của bạn.

Cộng tác hành chính

Lúc đầu, hợp tác hành chính không có vẻ như một thực hành an ninh. Làm thế nào có thể làm việc theo nhóm làm cho mạng nội bộ của bạn một nơi an toàn hơn?

Đầu tiên, hãy xem xét rằng bất kỳ hành động bất hợp pháp hoặc phi đạo đức liên quan đến các đối tác tự động có nghĩa là có người chứng kiến và có thể dẫn một cuộc điều tra. Như Benjamin Franklin đã từng nói, "Ba người có thể giữ bí mật nếu hai người trong số họ đã chết."

Thứ hai, xét trường hợp không có sự hợp tác rõ ràng trong một hoạt động đáng ngờ. Thực tế là có một quản trị viên khác, người có trách nhiệm đối với các hệ thống có liên quan có nghĩa là hệ thống chính nó đang được xem xét kỹ lưỡng. Thực tế là có sự giám sát của bên thứ ba của hệ thống có thể làm nản lòng những kẻ phạm tội trong trường hợp tốt nhất, hoặc ít nhất là dẫn đến việc khám phá các hoạt động đáng ngờ.

Tuy nhiên, bạn nên cẩn thận để tránh giao quá nhiều tay cho bất kỳ pot có được. Nó không chỉ có thể dẫn đến hệ thống hỗn loạn, mà nó cũng có thể làm cho

hoạt động phi đạo đức khó khăn hơn để theo dõi, trong một sự cố hoặc một cuộc kiểm toán.

Sản phẩm

Sản phẩm luôn thay đổi theo thời gian - bạn sẽ muốn kiểm tra các tạp chí công nghiệp mới nhất và các trang Web để đảm bảo rằng bạn đã có sự lựa chọn mới nhất trong phía trước của bạn.

- Quản lý máy tính để bàn
- Laptop / PDA An
- Bảo mật vật lý
- Quản lý nội dung

Tóm lược

Bảo mật nội bộ tốt chẳng khác gì việc bạn làm cho an ninh bên ngoài, và thực hành siêng năng liên quan đến tự kiểm toán và thực thi chính sách. Có những công cụ có thể giúp đỡ, chẳng hạn như các công cụ kiểm toán / máy quét an ninh, các công cụ lọc nội dung, quản lý máy tính để bàn, và IDS, nhưng trong phân tích cuối cùng, không có công cụ có thể thay thế cá nhân tỉ mỉ và tinh mắt.

Chương 7: Phân tích pháp y và Đáp ứng sự cố

Phân tích dữ liệu kỹ thuật

Phân tích pháp y không giống như nướng bánh, nhưng có một số điểm tương đồng. Nướng bánh là dễ dàng hơn nếu bạn xác định vị trí và tổ chức tất cả các thành phần đầu tiên. Nếu bạn đặt trứng của bạn, phủ sương giá, bơ, bột mì, và tất cả các thành phần khác được liệt kê trên các công thức trên quầy trước khi bạn bắt đầu, bạn có khả năng để nướng bánh tốt hơn trong một khoảng thời gian ngắn. Nguyên tắc này tương tự cho pháp y máy tính. Nếu bạn tập trung vào việc khai thác các dữ liệu trước khi bất kỳ giải thích, nó thường xuyên nuôi dưỡng một, phân tích pháp y toàn diện hơn hoàn toàn. Nó cũng có thể tiết kiệm thời gian.

Trong chương này, chúng tôi thảo luận làm thế nào để xác định vị trí và tổ chức tất cả các mảnh của phương tiện truyền thông máy tính và lắp ráp chúng trước khi bạn bắt đầu bất kỳ giải thích nội dung. Chúng tôi bao gồm các chủ đề sau:

- Khôi phục một nhân bản pháp y
- Khôi phục lại một hình ảnh pháp y có trình độ
- Phục hồi các tập tin đã xóa trước đó
- Phục hồi không gian chưa phân bổ và không gian chùng
- Tạo danh sách tập tin
- Thực hiện tìm kiếm chuỗi

Chuẩn bị cho phân tích pháp y

Chúng tôi đã thảo luận làm thế nào để tạo ra các bản sao pháp y và bản sao pháp y hạn chế của ổ đĩa cứng. Cả hai loại bản sao có thể yêu cầu thêm việc chuẩn bị theo yêu cầu để làm cho các thông tin mà chúng có có thể sử dụng. Cho dù bạn khôi phục lại bản sao hoặc phân tích nó ở định dạng gốc của nó hay không phụ thuộc vào nhiều yếu tố:

- Các phương pháp phân tích của tổ chức của bạn
- Các định dạng của dữ liệu gốc

- Các điều kiện của các dữ liệu ban đầu

Trước khi bạn có thể phân tích một nhân bản pháp y, bạn cần phải áp dụng các quy tắc của hệ thống tập tin gốc cho các tập tin ảnh. Những quy định này, thường được sử dụng bởi hệ điều hành gốc, cho phép truy cập vào hệ thống tập tin logic. Khi làm việc với các bản sao pháp y, điều này có thể được thực hiện theo ba cách.

- Ảnh bản sao có thể được phục hồi lên ổ đĩa khác, kết quả là một ảnh ánh xạ hay ảnh phục hồi. Sau đó bạn có thể sử dụng các công cụ DOS, chẳng hạn như các Maresware (www.maresware.com) hoặc các công cụ pháp y từ New Technologies, Inc. (www.forensics-intl.com).
- Bạn có thể phân tích các ảnh bản sao trong Linux, cho phép Linux để áp dụng các quy tắc hệ thống tập tin gốc cho ảnh bản sao.
- Bạn có thể cho phép một bộ công cụ pháp lý để thực hiện các chức năng của diễn giải, trình bày, kiểm tra việc nhân bản pháp y.

Phần tiếp theo là demo việc khôi phục pháp y trong các trường hợp:

- Khôi phục lại một bản sao pháp y
    - Khôi phục một Forensic sao chép của đĩa cứng
- Khôi phục một Forensic chép Qualified của đĩa cứng
    - *Khôi phục một bọc bằng chứng tin*
    - Khôi phục một SafeBack Evidence file
- Chuẩn bị một nhân bản pháp y để phân tích trong Linux
    - Kiểm tra việc Duplicate File Forensic
    - Gắn Duplicate File Forensic với các thiết bị Linux Loopback
- Rà soát các tập tin hình ảnh với bộ pháp y
    - Rà soát Duplicates Forensic trong EnCase
    - Rà soát Duplicates Forensic trong Forensic Toolkit
- Chuyển đổi một trùng lặp pháp y quaified để một bản sao pháp y
    - Phục hồi file bị xóa trên các hệ thống Windows
    - Sử dụng công cụ Windows-Based Để phục hồi tập tin trên hệ thống FAT file
    - Sử dụng Linux Công cụ phục hồi tập tin trên hệ thống FAT file
        - *Sử dụng FatBack để phục hồi tập tin bị xóa*
        - *Sử dụng TASK để phục hồi tập tin bị xóa*

    - Thực thi Autopsy như là một giao diện đồ họa cho File Recovery
    - Sử dụng Foremost để khôi phục các file bị mất
    - Phục hồi các file bị xóa trên hệ thống Unix
        - *Sử dụng debugfs để* nối lại *một tập tin* với Lost + *Found*
        - *Sử dụng debugfs để khôi phục các file bị xóa trước đây của dữ liệu chưa biết*
- Phục hồi không gian unallocated, không gian tự do, và không gian chùng

Tạo danh sách tập tin

Một trong những điều quan trọng nhất, để không bước nào bị bỏ qua trong việc phân tích nội dung của một ổ đĩa cứng là để tạo ra danh sách file tin thông tin. Những danh sách file này nên bao gồm các thông tin sau đây, ở mức tối thiểu:

- Đường dẫn đầy đủ mỗi file tìm thấy trong ổ đĩa chứng cứ
- Lần ghi và thay đổi thời gian/ngày cuối cùng cho mỗi file.
- Tạo nhãn thời giờ / ngày, nếu chúng tồn tại.
- Lần truy cập nhãn thời gian /ngày cuối cùng.
- Kích thước logic của mỗi tập tin.
- Băm MD5 của từng file.

Một số ví dụ:

- Bảng liệt kê tập tin Metadata
- Xác định được biết đến hệ thống tập tin
- Chuẩn bị một ổ đĩa để tìm kiếm chuỗi
- Thực hiện chuỗi Searches
    - *Thực hiện chuỗi tìm kiếm với Grep*
    - *Thực hiện chuỗi tìm kiếm với bọc*
    - *Thực hiện tìm kiếm chuỗi Sử dụng Task và khám*

Điều tra hệ thống Windows

Khi phản ứng sự cố ban đầu của bạn cho thấy rằng sự điều tra hơn nữa được bảo đảm, bạn có hai lựa chọn: Bạn có thể thực hiện các bước điều tra trên chính các phương tiện truyền thông bằng chứng, hoặc bạn có thể thực hiện bản

sao pháp y của các phương tiện truyền thông bằng chứng, và sau đó thực hiện các bước điều tra về một ảnh bản sao. Nếu bạn chọn để điều tra các phương tiện truyền thông bằng chứng trực tiếp mà không tạo ra một sự trùng lặp pháp y, bạn sẽ thay đổi các bằng chứng thực tế, và bạn sẽ không có một cơ sở để so sánh sau khi bước điều tra xâm nhập của bạn đã thay đổi hệ thống. Ví dụ, chỉ cần xem một tập tin hoặc thư mục mục trên hệ thống bằng chứng làm cho các thông tin về hệ thống bị thay đổi. Nhưng thông tin này có thể là yếu tố quan trọng trong việc thiết lập các hành vi của một nghi phạm.

Mặt khác, nếu bạn đã tạo ra một bản sao của các phương tiện truyền thông pháp y bằng chứng, bạn sẽ luôn luôn có hình ảnh pháp y ban đầu để khôi phục lại nếu các bước điều tra của bạn vô tình xóa hoặc phá hủy bằng chứng. Vì vậy, chúng tôi khuyên bạn nên sử dụng một nhân bản pháp y để điều tra của bạn.

Chương này nghiên cứu những cách khác nhau để điều tra hệ thống Windows (NT, 2000, và XP) trong một nỗ lực để khẳng định hành vi trái pháp luật, không thể chấp nhận, hoặc trái phép. Chúng tôi giả định rằng bạn đã thực hiện các nhiệm vụ sau:

- Thực hiện một phản ứng ban đầu và xác nhận rằng nghiên cứu thêm là cần thiết
- tham khảo ý kiến tư vấn pháp lý
- Thực hiện một sự trùng lặp pháp y của ổ đĩa bằng chứng, sử dụng Safeback, bọc, hoặc một công cụ chụp ảnh

Bạn sẽ cần một cách tiếp cận chính thức để điều tra hệ thống, bởi vì một cách tiếp cận có tổ chức sẽ dẫn đến những sai lầm và bị bỏ qua bằng chứng. Chương này vạch ra nhiều bước bạn sẽ cần phải thực hiện để tìm ra những bằng chứng để chứng minh hoặc bác bỏ cáo buộc.

Trường hợp bằng chứng cư trú trên các hệ thống Windows

Trước khi bạn đi sâu vào phân tích pháp y, điều quan trọng là phải biết được nơi bạn có kế hoạch để tìm kiếm các bằng chứng. Các địa điểm sẽ phụ thuộc vào từng trường hợp cụ thể, nhưng nói chung, chứng cứ có thể được tìm thấy trong các lĩnh vực sau:

- dữ liệu dễ bay hơi trong các cấu trúc hạt nhân
- không gian Slack, nơi bạn có thể có được thông tin từ các tập tin đã xóa trước đó được phục hồi được
- Miễn phí không gian hoặc chưa được chia, nơi bạn có thể có được các tập tin đã xóa trước đó, bao gồm cả các cụm bị hư hỏng hoặc không thể tiếp cận
- Các hệ thống tập tin hợp lý
- Các bản ghi sự kiện
- Các Registry, mà bạn nên nghĩ đến như là một file log lớn
- Áp dụng các bản ghi không được quản lý bởi Windows Event Log Dịch vụ
- Các tập tin hoán đổi, mà chứa thông tin gần đây đã được đặt trong hệ thống RAM (pagefile.sys có tên trên phân vùng hoạt động)
- tập tin ứng dụng cấp đặc biệt, chẳng hạn như các tập tin lịch sử Internet Internet Explorer (index.dat), fat.db Netscape, các tập tin history.hst, và bộ nhớ cache của trình duyệt
- Các file tạm thời được tạo ra bởi nhiều ứng dụng
- Các Recycle Bin (a, cấu trúc tập tin hợp lý tiềm ẩn nơi các mặt hàng gần đây đã xóa có thể được tìm thấy)
- Các ống máy in
- Đã gửi hoặc nhận email, chẳng hạn như các tập tin .pst của Outlook email

Trong một cuộc điều tra, bạn có thể cần phải tìm kiếm các bằng chứng trong mỗi lĩnh vực, trong đó có thể là một quá trình phức tạp. Chúng tôi sẽ phác thảo một khuôn khổ điều tra trong chương này.

Tiến hành một cuộc điều tra của Windows

Sau khi bạn đã thiết lập máy trạm pháp y của bạn với các công cụ thích hợp và ghi lại các dữ liệu phân vùng cấp thấp từ các hình ảnh mục tiêu, bạn đã sẵn sàng để tiến hành điều tra. Các bước điều tra cơ bản sau đây được yêu cầu cho một cuộc kiểm tra chính thức của một hệ thống mục tiêu:

- Xem xét tất cả các bản ghi thích hợp.
- Thực hiện tìm kiếm từ khóa.
- Xem xét các tập tin có liên quan.

- Xác định các tài khoản người dùng hoặc nhóm trái phép.
- Xác định its quá trình and other dịch vụ giả mạo.
- Tìm kiếm các tập tin bất thường hoặc ẩn / thư mục.
- Kiểm tra các điểm truy cập trái phép.
- Kiểm tra việc chạy bởi dịch vụ Scheduler.
- Phân tích các mối quan hệ tin tưởng.
- Xem lại định danh bảo mật.

Các bước này không sắp xếp theo thời gian hoặc theo thứ tự quan trọng. Bạn có thể cần phải thực hiện từng bước hay chỉ là một vài trong số họ. Cách tiếp cận của bạn phụ thuộc vào kế hoạch phản ứng của bạn và hoàn cảnh của vụ việc.

Rà soát tất cả các bản ghi thích hợp

Các hệ điều hành Windows NT, 2000, và XP duy trì ba tập tin log riêng biệt: log hệ thống, log ứng dụng, log bảo mật. Bằng cách xem xét các bản ghi này, bạn có thể để có được những thông tin sau đây:

- Xác định những người dùng đã được truy cập vào các tập tin cụ thể
- Xác định những người đã thành công đăng nhập vào hệ thống
- Xác định những người đã cố gắng không thành công để đăng nhập vào một hệ thống
- sử dụng Theo dõi của các ứng dụng cụ thể
- Theo dõi các thay đổi chính sách kiểm toán
- Theo dõi các thay đổi cho phép người sử dụng (ví dụ như tăng truy cập)

Các tiến trình hệ thống và các hoạt động điều khiển thiết bị được ghi lại trong nhật ký hệ thống. Sự kiện hệ thống kiểm toán bởi Windows bao gồm trình điều khiển thiết bị mà không bắt đầu đúng cách; lỗi phần cứng; trùng lặp địa chỉ IP; và bắt đầu, tạm dừng, và dừng dịch vụ.

Thực hiện tìm kiếm theo từ khóa

Trong cuộc điều tra về sở hữu tài sản trí tuệ hoặc thông tin độc quyền, tội phạm tình dục, và bất kỳ trường hợp thực tế liên quan đến truyền thông dựa trên văn bản, điều quan trọng là phải thực hiện tìm kiếm chuỗi các ổ đĩa cứng của đối tượng. Nhiều từ khóa khác nhau có thể là rất quan trọng để điều tra, bao gồm cả

các ID người dùng, mật khẩu, dữ liệu nhạy cảm (từ mã), tên tập tin được biết đến, và từ môn học cụ thể (ví dụ, cần sa, mary jane, bong, và dope). Có thể tìm kiếm chuỗi được thực hiện trên cấu trúc tập tin logic hoặc ở mức vật lý để kiểm tra nội dung của toàn bộ ổ đĩa.

Hầu hết các công cụ đĩa tìm kiếm được thị trường như là phần mềm pháp y thực hiện liệu đọc từ ổ đĩa cứng, tiến hành một chuỗi tìm kiếm cấp vật lý của ổ đĩa. Những loại công cụ này yêu cầu bạn khởi động hệ thống mục tiêu từ một đĩa mềm khởi động kiểm soát hoặc các phương tiện khác (họ không thể chạy từ ổ đĩa cứng đang hoạt động) và chạy công cụ, bởi vì bạn không thể đọc phất lý một ổ đĩa đang chạy một hệ điều hành Windows.

Rà soát các tập tin liên quan

Xác định các tập tin chứa chấp bằng chứng của một cuộc tấn công hoặc sử dụng sai trên hệ thống Windows có thể là một nhiệm vụ nặng nề, thú vị, và khó khăn. Thường có dấu vết bằng chứng ở đâu đó trên hệ thống giúp để xác nhận hoặc xua tan những nghi ngờ của bạn. Phần cứng có thể tìm thấy nó.

Hệ thống Windows ghi đầu vào và đầu ra rất nhiều tập tin tại một thời điểm mà hầu như tất cả các hành động thực hiện trên hệ thống để lại một số dấu vết của sự xuất hiện của chúng. Windows có các file tạm, các file cache, một Registry mà theo dõi các file vừa sử dụng, một Recycle Bin duy trì các tập tin bị xóa, và vô số các địa điểm khác, nơi dữ liệu thời gian chạy được lưu trữ.

Điều quan trọng là nhận ra các tập tin bằng phần mở rộng của chúng cũng như tiêu đề tập tin thực sự của họ (nếu có thể). Ở mức tối thiểu, bạn cần phải biết những file .doc, .tmp, .log, .txt, .wpd, .gif, .exe, và các tập tin .jpg là gì. Bạn có thể khai thác các định dạng khác:

- Netscape Messenger Mail
- Microsoft Outlook Mail
- Undelete Tools
- The Recycle Bin
- Temporary Files
- Backup File Recovery
- The Registry on a Live System
- The Registry Offline

- Netscape and Internet Explorer History Files

Xác định tài khoản người dùng trái phép hoặc Groups

Một thủ đoạn phổ biến của kẻ gian là khởi tạo các tài khoản giả mạo trên hệ thống hoặc để nâng cao đặc quyền của họ đến một mức độ trái phép, nơi họ có thể có được dữ liệu mà họ không nên có thể truy cập. Có một số cách để kiểm toán các tài khoản người dùng và nhóm người dùng trên một hệ thống sống:

- Tìm trong User Manager cho các tài khoản người sử dụng trái phép (trong khi một hệ thống phản ứng trực tiếp).
- Sử dụng `usrstat` từ NTRK để xem tất cả các tài khoản tên miền trên một bộ điều khiển tên miền, tìm kiếm mục đáng ngờ.
- Kiểm tra các bản ghi Security sử dụng Event Viewer, lọc cho sự kiện ID 624 (thêm một tài khoản mới), 626 (tài khoản người dùng kích hoạt), 636 (thay đổi một nhóm tài khoản), và 642 (tài khoản người dùng đã thay đổi).
- Kiểm tra \% systemroot% \ Profiles thư mục trên hệ thống. Nếu các tài khoản người dùng tồn tại, nhưng không có tương ứng \% systemroot% \ Profiles \ <useraccount> thư mục, mà tài khoản người dùng đã không được sử dụng để đăng nhập vào hệ thống được nêu. Nếu thư mục đó không tồn tại, nhưng các tài khoản người dùng không còn được liệt kê trong quản lý tài khoản hoặc Registry (tại HKLM \ SAM \ Domains \ Account \ Users \ Tên), mà ID người dùng đã tồn tại một thời gian nhưng không còn tồn tại.
- Xem xét các SID trong Registry, dưới HKLM \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ ProfileList. Khi một tài khoản người dùng bị xóa, các mục hồ sơ thư mục tương ứng là không bị xóa, và SID tương ứng sẽ ở lại trong Registry, như thể hiện trong hình minh họa sau đây (trong đó Registry thấy một giá trị SID tồn tại cho người sử dụng ID mandingo, mà không còn tồn tại như một tài khoản người dùng hợp lệ trên hệ thống). Điều này cho phép bạn theo dõi mà ID người dùng đã bị xóa trong quá trình cuộc sống của một hệ thống.

Xác định tiến trình Rogue

Xác định tiến trình rogue là đơn giản hơn nhiều khi xem xét một hệ thống đang chạy. Do hầu hết các tiến trình rogue lắng nghe cho các kết nối mạng hoặc sniff mạng cho ID người dùng và mật khẩu dạng cleartext, các tiến trình này dễ dàng hơn để tìm thấy khi họ đang thực hiện.

Giải pháp đơn giản nhất là để chạy quét virus cập nhật nhất trên toàn bộ dung lượng logic của chứng cứ. Nếu bạn chọn để chạy một tiện ích kiểm tra virus đối với các hệ thống tập tin của hình ảnh được khôi phục, cần đảm bảo rằng khối lượng được gắn quyền chỉ đọc. Bạn sẽ không muốn các công cụ bắt đầu di chuyển và xóa các tập tin mà bạn không biết! Một công cụ tuyệt vời để nhận dạng các trojan, backdoor, keystroke logger, và "phần mềm độc hại" khác là PestPatrol. Xem xét sử dụng công cụ này để tìm kiếm các file hệ thống.

Tìm kiếm file bất thường hoặc bị ẩn

NTFS có một tính năng, ban đầu được phát triển trên Macintosh Hierarchical File System (HFS), để lưu trữ nhiều trường hợp của tập tin dữ liệu dưới một mục file. Những nhiều luồng dữ liệu có thể được sử dụng để ẩn dữ liệu, bởi vì Windows Explorer không cho thấy sự hiện diện của các dòng bổ sung.

Kiểm tra cho các điểm truy cập trái phép

Một trong những khác biệt lớn nhất giữa Windows NT và các hệ thống Unix là NT không cho phép truy cập cấp độ dòng lệnh từ xa qua mạng mà không có việc sử dụng các tiện ích bên ngoài. Điều này đã thay đổi đáng kể với Windows 2000, cái đi kèm với một máy chủ Telnet cho quản trị lệnh từ xa. Bất kỳ dịch vụ cho phép một mức độ truy cập từ xa có thể cung cấp một điểm vào những kẻ xâm nhập không mong muốn. Ngoài xây dựng và trong các ứng dụng của bên thứ ba, trojan có thể cung cấp dịch vụ đó. Những dịch vụ này bao gồm những điều sau đây:

- Máy chủ terminal
- SQL/Oracle
- daemon telnet của bên thứ ba trên Windows NT
- Windows 2000 Telnet Server
- Third-party FTP daemon

- máy chủ Web (chẳng hạn như Apache và IIS)
- tính toán mạng ảo (TCP port 5800) và PC Anywhere (cổng TCP 5631)
- Dịch vụ truy cập từ xa (PPP và PPTP)
- X Servers

Phân tích mối quan hệ tin cậy

Các mối quan hệ tin cậy giữa các lĩnh vực chắc chắn có thể tăng phạm vi của một thỏa hiệp nên một ID và mật khẩu người dùng hợp lệ bị đánh cắp bởi một kẻ tấn công. Truy cập vào một máy có thể có nghĩa là truy cập hợp lý cho nhiều người khác. Các mối quan hệ tin tưởng có thể làm tăng phạm vi của một thỏa hiệp và nâng cao mức độ nghiêm trọng của vụ việc. Thật không may, việc xác định sự tin tưởng trong miền Windows là không đơn giản như nó đang ở trong môi trường Unix.

Rà soát chứng nhận bảo mật (SID)

Để thiết lập các hành động của một ID người dùng cụ thể, bạn có thể cần phải so sánh SIDs tìm thấy trên máy nạn nhân với những người có thẩm quyền chứng thực trung tâm. Chúng tôi đã đề cập đến SIDs trước đó trong chương này. Ở đây, chúng tôi giải thích như thế nào SIDs có thể đóng góp để ứng phó sự cố.

SID được sử dụng để xác định một người dùng hoặc một nhóm duy nhất. Mỗi hệ thống có nhận dạng riêng của mình, và mỗi người dùng có nhận dạng riêng của mình trên hệ thống đó. Từ định tính và định danh người dùng được kết hợp để làm cho các SID. Như vậy, SID duy nhất có thể xác định tài khoản người dùng. SIDs không áp dụng để chia sẻ an ninh.

Tập kiểm toán và đánh cắp thông tin

Khi cài đặt Windows NT, bạn có thể chọn giữa việc sử dụng hệ thống tập tin FAT hoặc các hệ thống tập tin NTFS. Nếu một trang web mong muốn thực hiện kiểm toán các truy cập tập tin cụ thể, nó cần NTFS. Các hệ thống tập tin NTFS cho phép bạn tạo danh sách điều khiển truy cập (ACL) cho các thư mục và tập tin trên một hệ thống. Do đó, NTFS được coi là một hệ thống tập tin an toàn hơn so với FAT cũ đồng bằng hoặc FAT32. Nếu bạn cần phải xác định những người có quyền truy cập vào những gì trên hệ thống, DumpSec, một công cụ miễn

phí của SomarSoft, kiểm tra các ACL của các tập tin và thư mục và tạo ra một phác thảo của các nguồn tài nguyên, các nhóm, và cấp độ truy cập.

Xử lý các nhân viên rời

Khi một thành viên chủ chốt của nhóm nghiên cứu lá bất ngờ, các chính sách và thủ tục cần phải được thực hiện để bảo vệ công ty, cũng như các cá nhân những người còn lại. Ở đây, chúng tôi khám phá một số bước đơn giản cho việc xác định nhân viên rời được bước ra khỏi cửa với các thông tin có giá trị.

Rà kiếm và Files Được sử dụng

Một trong những bước đầu tiên phải thực hiện khi một nhân viên rời khỏi công ty là để xem những gì các số tìm kiếm cuối cùng trên hệ thống của mình đã. Một cách đơn giản để làm điều này là nhìn vào hộp cuộn trong hộp thoại Find.

Tiến hành chuỗi kiếm trên ổ đĩa cứng

Một tùy chọn khác để kiểm tra những gì một sớm-to-be cựu nhân viên đã và đang làm là chuẩn bị một đĩa khởi động để thực hiện tìm kiếm chuỗi trên một ổ đĩa cứng. Các danh sách từ phải được xây dựng một cách cẩn thận, có tính đến những thông tin cá nhân đã tiếp cận và những điều nhân viên không nên thấy.

Bạn có thể có một đĩa mềm khởi động điều khiển duy nhất với DtSearch hoặc tiện ích stringsearch khác và duy trì một danh sách các mã chủ chốt của dự án, khách hàng chủ chốt, và dữ liệu của công ty mà bạn không muốn có "rò rỉ" từ tổ chức của bạn.

Điều tra hệ thống Unix

Hệ điều hành Unix mạnh mẽ, mềm dẻo. The functionality that makes it so useful also makes it a challenge to protect and investigate. This chapter outlines the features of the Unix operating system that are most likely to aid the investigator in determining the who, what, when, where, and how of an incident. We present the investigative techniques in as forensically a sound manner as possible. At this point of the investigation, we assume that you have performed an initial response. You will use the data you collected during the initial response for the investigative steps covered in this chapter.

Keep in mind that this chapter cannot cover every possible Unix incident. Critical thinking skills and a fundamental understanding of the functionality of Unix are necessary for a truly effective response.

Tổng quan về các bước trong một cuộc điều tra Unix

Một khi bạn đã sẵn sàng để bắt đầu điều tra các hệ thống Unix, các hành động sau đây cung cấp những cách chắc chắn nhất để xác định chứng cứ có liên quan:

- Xem xét tất cả các bản ghi thích hợp
- Thực hiện tìm kiếm từ khóa
- Xem xét các tập tin có liên quan
- Xác định các tài khoản người dùng hoặc nhóm trái phép
- Xác định các quá trình lừa đảo
- Kiểm tra các điểm truy cập trái phép
- Phân tích các mối quan hệ tin tưởng
- Kiểm tra các mô-đun hạt nhân rootkit

Các bước này không được liệt kê theo thời gian hoặc theo thứ tự quan trọng. Bạn có thể không cần phải thực hiện tất cả các bước này cho mỗi sự cố. Cách tiếp cận của bạn phụ thuộc vào sự cố cụ thể và các mục tiêu phản ứng của bạn.

Khi bạn tiến hành điều tra của mình, ý thức được rằng, trong trường hợp có sự thỏa hiệp root, bất cứ điều gì có thể xảy ra. Một kẻ tấn công có quyền root cho một hệ thống có thể thay đổi bất cứ thứ gì trên hệ điều hành, bao gồm cả các bằng chứng mà bạn đang xem xét. Ví dụ, khi một tập tin log không chứa một mục mà chứng thực bằng chứng khác, hãy nhớ rằng kẻ tấn công có quyền truy cập root có thể đã bị xóa các entry file log. Ngược lại, nếu hệ thống nạn nhân có bằng chứng của một sự xâm nhập thành công từ một nguồn địa chỉ IP cụ thể, nó có thể là một kẻ tấn công có quyền truy cập root "trồng" bằng chứng đó.

Chương 8: phục hồi sự cố

Khôi phục từ một sự cố an ninh

Bây giờ bạn đã trả lời một sự cố an ninh, và có cả bằng chứng thu thập và bảo quản của một cuộc tấn công, bạn phải giúp công ty của bạn trở lại làm việc. Các nhanh hơn và hiệu quả hơn, bạn có thể phục hồi từ một sự cố an ninh, thiệt hại tài chính ít hơn là phải chịu đựng, và càng có nhiều khả năng công ty có thể ngăn chặn sự cố tương tự xảy ra. Để phục hồi hoàn toàn từ sự kiện này, bạn không những phải biết làm thế nào để sửa chữa hệ thống mạng, mà còn làm thế nào để mô tả các vấn đề để các nhà hoạch định chính tại công ty bạn để sự cố trong tương lai có thể tránh được.

Basic Incident phục hồi Process

Quá trình cơ bản cho việc phục hồi sự cố là tương đối đơn giản:

1. Đánh giá mức độ thiệt hại gây ra bởi vụ việc.

2. Khôi phục từ sự kiện này.

3. Báo cáo vụ việc.

Đánh giá thiệt hại

Trong hoặc sau một sự cố an ninh, đánh giá thiệt hại nên được thực hiện để xác định mức độ thiệt hại, nguồn gốc hay nguyên nhân của vụ việc, và số lượng thời gian chết mong đợi. Việc đánh giá cũng có thể xác định các chiến lược phù hợp để sử dụng khi bạn di chuyển vào giai đoạn phục hồi.Recovery Methods

Sau khi đánh giá thiệt hại, bạn sẽ biết được mức độ phục hồi mà cần phải được thực hiện. Nhiều tổ chức dựa trên định dạng hệ thống trong trường hợp của một cuộc tấn công mã rootkit, áp dụng các bản vá lỗi phần mềm hoặc tải lại phần mềm hệ thống trong trường hợp của một virus hoặc mã độc hại phá hoại, và khôi phục lại bản sao lưu trong trường hợp của một sự xâm nhập hay tấn công backdoor. Phương pháp phục hồi cũng có thể involvereplacing phần cứng trong trường hợp của một sự cố an ninh vật lý.

.

Incident Report

Section 1: Incident Description

Date and time detected: _____ Date and time reported: _____
Location: _____ Name of first responder: _____
System or application affected: _____ Title of first responder: _____
Name and contact information for other responders: _____ Contact information for first responder: _____

Section 2: Summary of Incident

Incident type detected:

❒ DoS	❒ Unplanned downtime
❒ Unauthorized access or use	❒ Damage to hardware
❒ Malicious code	❒ Other

Tools used to detect the incident: _____

Detailed incident description: _____

Section 3: Notification and Escalation

❒ IS Team	❒ Public Affairs
❒ Local law enforcement	❒ Government regulatory agencies

Báo cáo sự cố

Báo cáo sự cố là một báo cáo bao gồm một mô tả về những sự kiện đã xảy ra trong một sự cố an ninh. Nên cẩn thận để viết càng nhiều chi tiết liên quan đến một vụ việc càng tốt, chẳng hạn như tên gọi của tổ chức, bản chất của các sự kiện, tên và số điện thoại liên lạc, thời gian và ngày của một sự kiện, và thông tin đăng nhập. Tuy nhiên, một báo cáo không nên trì hoãn vì những vấn đề với việc thu thập thông tin. Đầu dò có thể tiếp tục được tiến hành sau khi báo cáo đã được viết ra.

Hướng dẫn khôi phục sự cố bảo mật

Đánh giá thiệt hại, phục hồi, và báo cáo rất quan trọng trong việc đối phó với một sự cố. Thực hiện theo các hướng dẫn chung trong quá trình phục hồi tổng thể:

- Một số bước bạn có thể mất trong khi đánh giá thiệt hại trong một sự cố an ninh
    - Đánh giá các khu vực thiệt hại để xác định các khóa học tiếp theo của hành động.
    - Xác định số tiền thiệt hại cho các cơ sở, phần cứng, hệ thống và mạng lưới.
    - Nếu công ty của bạn đã bị kỹ thuật số chứ không phải vật lý thiệt hại, bạn có thể cần phải kiểm tra các tập tin log, xác định các tài khoản đã bị xâm nhập, và xác định các tập tin đã được sửa đổi trong cuộc tấn công.
    - Nếu công ty của bạn đã bị vật lý và kỹ thuật số không-thiệt hại, bạn có thể cần phải kiểm kê vật lý để xác định các thiết bị đã bị đánh cắp hoặc bị hư hỏng, trong đó khu vực các kẻ xâm nhập (s) có thể truy cập, và bao nhiêu thiết bị có thể có được bị hư hỏng hoặc bị đánh cắp.
    - Một trong những thành phần quan trọng nhất và bỏ qua các đánh giá thiệt hại là để xác định xem việc tấn công trở lên; cố gắng để đối phó với một cuộc tấn công vẫn đang được tiến hành có thể làm hại nhiều hơn lợi.
- Một số bước bạn có thể thực hiện khi hồi phục từ một sự cố an ninh:

- Thay thế phần cứng và mạng cáp trong trường hợp nào đã bị hư hỏng hoặc bị đánh cắp.
- Phát hiện và xóa các phần mềm độc hại và vi rút từ các hệ thống và phương tiện truyền thông bị ảnh hưởng.
- Ngắt kết nối các hệ thống bị xâm nhập từ các máy chủ và tắt máy chủ để tránh sự xâm nhập sâu hơn.
- Vô hiệu hoá quyền truy cập vào tài khoản người dùng đã bị ảnh hưởng mạng và tìm kiếm cho tất cả các phần mềm backdoor được cài đặt bởi các kẻ xâm nhập.
- Thiết lập mà tổ chức của bạn không còn được tiếp xúc với một mối đe dọa bằng cách quét các mạng và hệ thống sử dụng một IDS.
- Kết nối lại các máy chủ mạng.
- Khôi phục dữ liệu và hệ thống mạng từ backup gần đây nhất.
- Thay thế dữ liệu bị xâm nhập và các ứng dụng, hoặc định dạng lại hệ thống và thực hiện cài đặt mới của hệ điều hành.
- Cứng mạng và máy chủ bằng cách thay đổi mật khẩu, cài đặt các bản vá lỗi, và đặt lại cấu hình tường lửa và router.
- Thông báo cho cán bộ công ty và các bên liên quan quan trọng của vụ việc, và nếu một người trong cuộc là nguồn gốc của sự việc, khiển trách cá nhân phụ trách theo chính sách công ty, hoặc thực thi pháp luật liên hệ để có hành động tùy thuộc vào mức độ của cuộc tấn công.
- Viết một báo cáo mô tả các quá trình phục hồi. Một bản tóm tắt của báo cáo này nên được lưu để sử dụng trong phản ứng sự cố an ninh trong tương lai.

- Một số chi tiết bạn có thể cần phải nắm bắt khi báo cáo một sự cố an ninh:
  - Tên của tổ chức.
  - Họ tên và số điện thoại của người phát hiện vụ việc.
  - Tên (s) và số điện thoại (s) của phản ứng đầu tiên (s)
  - Các loại sự kiện; Ví dụ, một cuộc tấn công vật lý, tấn công mã độc hại, hoặc tấn công mạng.
  - Ngày và thời gian của sự kiện, bao gồm múi giờ.

- Các nguồn và đích của hệ thống và mạng lưới, bao gồm địa chỉ IP.
- Các hệ điều hành and phần mềm chống vi rút used, and other version of their.
- Các phương pháp được sử dụng để phát hiện sự cố; Ví dụ, các bản ghi hoặc IDS.
- Các tác động kinh doanh của vụ việc.
- Các bước giải quyết lấy.

Kinh doanh liên tục

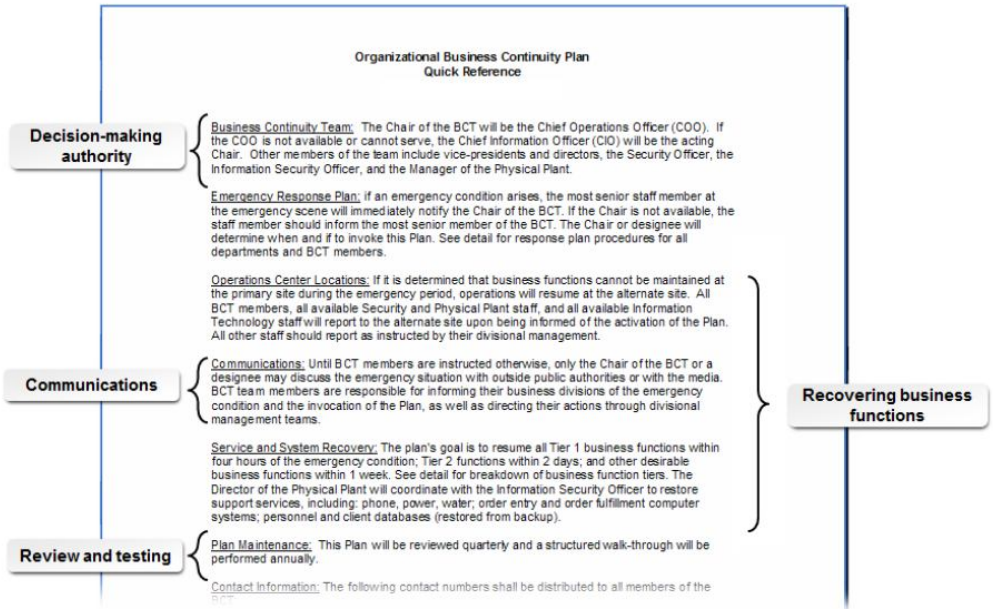
Bạn sẽ cần phải phát triển BCPS và DRPs để giúp giảm thiểu thiệt hại ở tổ chức của bạn. Là một chuyên gia bảo mật, bạn cần phải đi lên với những kế hoạch tốt nhất có thể. Trong chủ đề này, bạn sẽ mô tả tầm quan trọng của kinh doanh liên tục cho một tổ chức.

Một hệ thống bảo mật chỉ là tốt như khả năng của mình để tránh khỏi các mối đe dọa và khắc phục thiên tai. Do đó, một thành phần quan trọng của hệ thống đó là phải có một kế hoạch tại chỗ để khi xảy ra thảm họa, doanh nghiệp sẽ vẫn tiếp tục trong thời cho đến khi vấn đề được cố định. Một BCP sẽ giúp đảm bảo dịch vụ liên tục cho khách hàng. Là một chuyên gia bảo mật, bạn có thể không chịu trách nhiệm về tính liên tục kinh doanh tổng thể, nhưng bạn sẽ là một đóng góp quan trọng đối với các thành phần an ninh và kế hoạch, do đó, một sự hiểu biết tốt về các kế hoạch, các thành phần của nó, và quá trình mà nó được xây dựng là quan trọng.

BCPs

Một kế hoạch kinh doanh liên tục (BCP) là một chính sách định nghĩa như thế nào một tổ chức sẽ duy trì hoạt động kinh doanh hằng ngày bình thường trong trường hợp gián đoạn kinh doanh hoặc khủng hoảng. Một BCP khả thi nên liên quan đến việc xác định các hệ thống quan trọng và các thành phần để đảm bảo rằng tài sản đó được bảo vệ. Các BCP cũng đảm bảo sự sống còn của các tổ chức chính nó bằng cách bảo quản tài liệu quan trọng, thiết lập quyền ra quyết định, giao tiếp với các bên liên quan trong và ngoài nước, và duy trì các chức năng tài chính. Các BCP nên giải quyết các vấn đề cơ sở hạ tầng như duy trì dịch vụ tiện

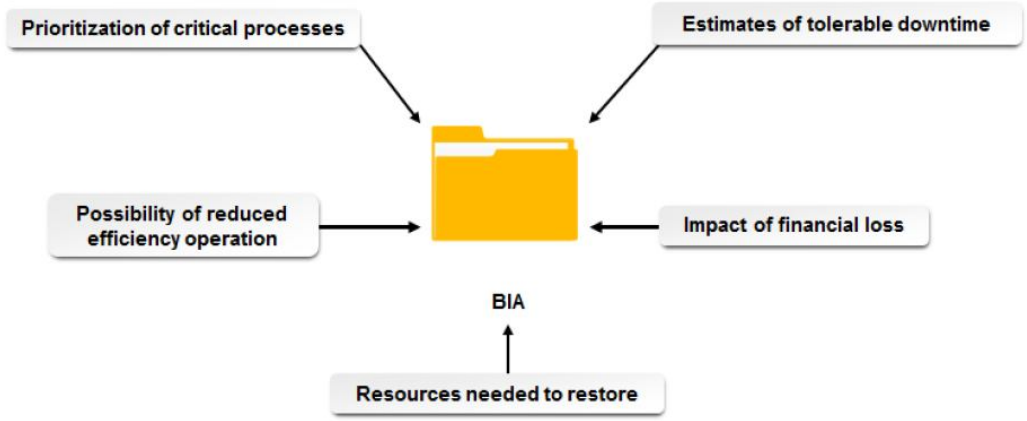
ích, sử dụng cao có sẵn hoặc các hệ thống chịu lỗi có thể chịu được sự thất bại, và việc tạo ra và duy trì các bản sao lưu dữ liệu. Các BCP nên được xem xét và kiểm tra một cách thường xuyên. Các kế hoạch phải có hỗ trợ điều hành được coi là độc quyền; các hành ủy quyền cá nhân phải ký kế hoạch.



Một BCP.

BIA

Một phân tích tác động kinh doanh (BIA) là một bước chuẩn bị trong phát triển BCP để nhận biết rủi ro của tổ chức hiện tại và xác định tác động đến hoạt động kinh doanh quan trọng đang diễn ra và xử lý rủi ro nếu như thực sự xảy ra. Bias chứa đánh giá tính dễ tổn thương và đánh giá để xác định rủi ro và tác động của chúng. Thiên vị nên bao gồm tất cả các giai đoạn của doanh nghiệp để đảm bảo một chiến lược tiếp tục kinh doanh mạnh mẽ.



Như một rủi ro được xác định, một tổ chức xác định các cơ hội nguy cơ xuất hiện và sau đó xác định số lượng thiệt hại của tổ chức tiềm năng. Ví dụ, nếu một cây cầu đường bộ băng qua một con sông địa phương được rửa sạch bởi một lũ và nhân viên không thể đạt được một cơ sở kinh doanh trong năm ngày, chi phí ước tính cho tổ chức cần phải được đánh giá về nhân lực bị mất và sản xuất.

MTD

Thời gian chết có thể chịu được tối đa (MTD) là khoảng thời gian dài nhất của thời gian mà một cúp doanh nghiệp có thể xảy ra mà không gây ra sự thất bại kinh doanh không thu hồi được. Mỗi quá trình kinh doanh có thể có MTD riêng của mình, chẳng hạn như một loạt các phút đến vài giờ cho các chức năng quan trọng, 24 giờ cho các chức năng khẩn cấp, 7 ngày đối với các chức năng bình thường, và như vậy. MTDs khác nhau tùy theo công ty và sự kiện.

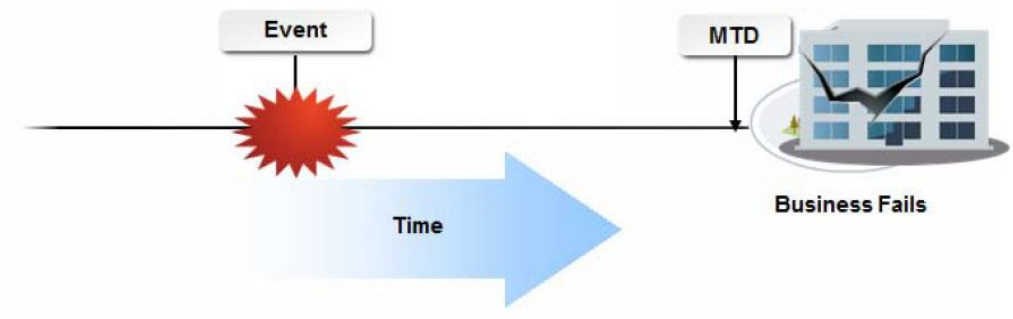
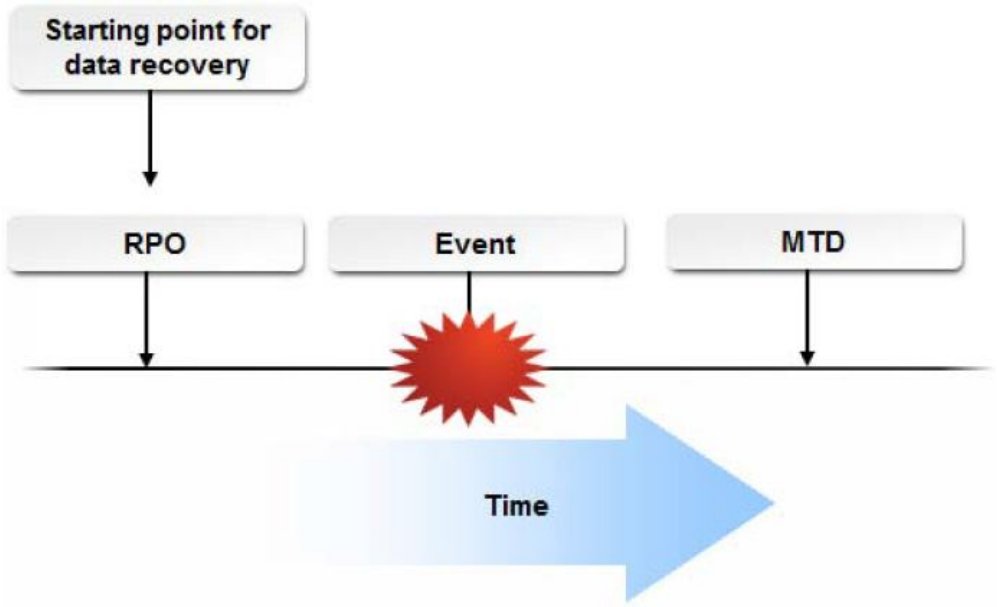


Figure 8-3: MTD.

Các MTD giới hạn số lượng thời gian phục hồi mà một doanh nghiệp có tiếp tục hoạt động. Ví dụ, một tổ chức chuyên về thiết bị y tế có thể tồn tại mà không có nguồn cung cấp sản xuất đến ba tháng vì nó đã dự trữ hàng tồn kho khá lớn. Sau ba tháng, tổ chức sẽ không có đủ nguồn cung cấp và có thể không có khả năng để sản xuất các sản phẩm bổ sung, do đó, dẫn đến thất bại. Trong trường hợp này, MTD là ba tháng.

RPO

Mục tiêu điểm khôi phục (RPO) là điểm trong thời gian, liên quan đến một thảm họa, nơi mà quá trình phục hồi dữ liệu bắt đầu. Trong các hệ thống IT, nó thường là thời điểm khi sao lưu thành công cuối cùng được thực hiện trước khi một sự kiện gây rối xảy ra.

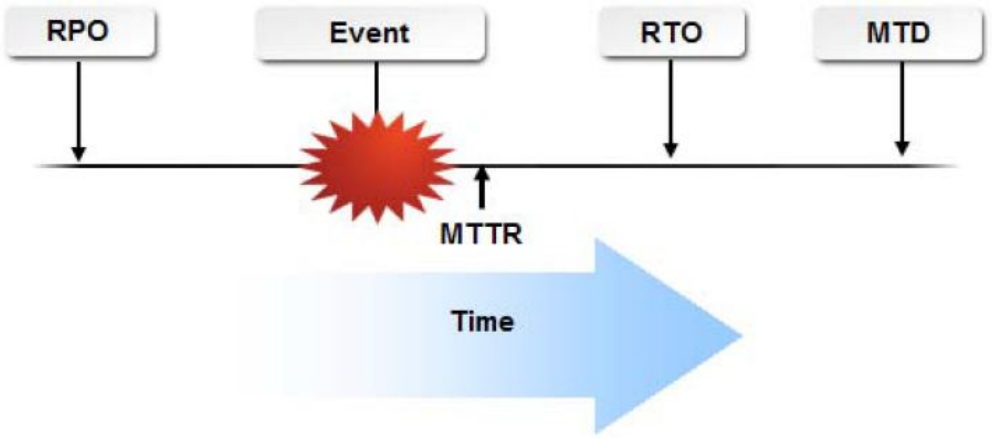


Một RPO.

Ví dụ, nếu sao lưu cuối cùng đã được thực hiện vào buổi chiều chủ nhật và thất bại xảy ra vào ngày thứ ba sau đây, thì RPO là buổi chiều chủ nhật. Các sao lưu mới nhất được khôi phục và xử lý bắt đầu hồi phục tất cả các hoạt động từ chiều chủ nhật để các điểm thất bại thứ ba.

RTO

Thời gian phục hồi quan (RTO) là chiều dài của thời gian mà hoạt động kinh doanh thông thường và các hoạt động có thể được phục hồi sau một sự xáo trộn. Nó bao gồm thời gian phục hồi cần thiết để trở về RPO và phục hồi lại hệ thống và tiếp tục chế biến từ trạng thái hiện tại của nó. Các RTO phải đạt được trước khi MTD. Thời gian để phục hồi (MTTR) có nghĩa là thời gian trung bình thực hiện cho một doanh nghiệp để phục hồi từ một sự cố hay thất bại và là một bù đắp của RTO. Nếu MTTR vượt RTO đưa ra, thì hoạt động kinh doanh cần phải chuyển sang các trang web thay thế.



Một RTO.

Tính liên tục của Kế hoạch hoạt động

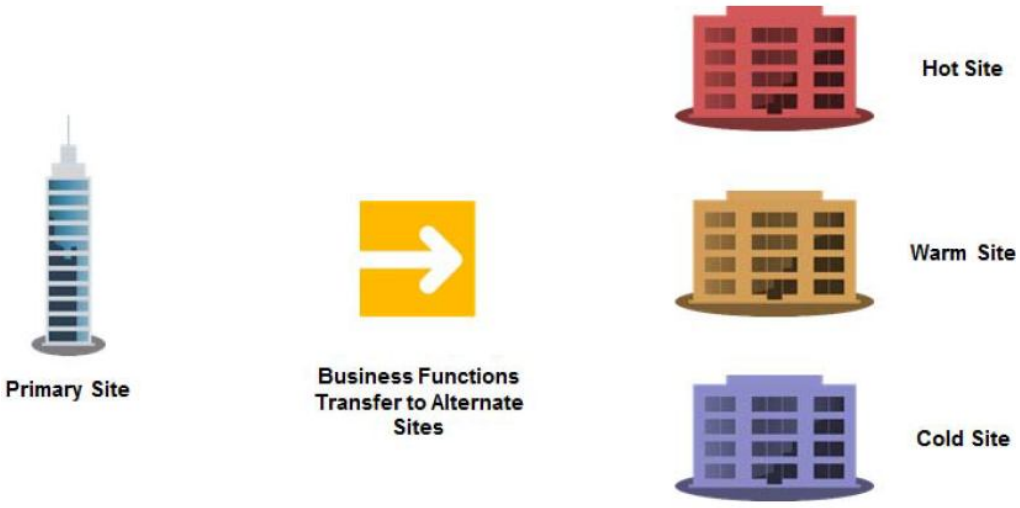
Một tục của hoạt động kế hoạch là thành phần của BCP cung cấp thực hành tốt nhất để giảm thiểu rủi ro và các biện pháp tốt nhất để phục hồi từ các tác động của một sự cố. An liên tục có hiệu quả của các hoạt động kế hoạch có thể bao gồm:

- Kiểm toán các nguồn tài nguyên, nhân viên và quản lý hoạt động.
- Thiết bị lưu trữ Kiểm toán, trung tâm dữ liệu, hệ điều hành, và các phần mềm và ứng dụng.
- Mạng Kiểm toán chẳng hạn như các mạng cục bộ (LAN) và mạng diện không dây (WAN), bao gồm truy cập từ xa và hệ thống xác thực.
- Phân tích rủi ro toàn diện và dễ bị tổn thương.
- Tạo bản sao lưu dữ liệu, phương pháp phục hồi, và thủ tục ứng phó khẩn cấp.
- Thiết lập quy trình về quản lý hoạt động trong một thảm họa.

Các bước trong một tính liên tục của hoạt động kế hoạch.

Các site thay thế

Là một phần của một BCP, một tổ chức có thể duy trì nhiều loại của các trang web khác mà có thể được sử dụng để khôi phục lại chức năng hệ thống. Một trang web nóng là một mạng thay thế đầy đủ cấu hình mà có thể được trực tuyến một cách nhanh chóng sau một thảm họa. Một trang web ấm là một địa điểm đó là không hoạt động hoặc thực hiện các chức năng không quan trọng trong điều kiện bình thường, nhưng mà có thể nhanh chóng chuyển đổi sang một trang web hoạt động chính nếu cần thiết. Một trang web lạnh là một vị trí thay thế được xác định trước, nơi một mạng có thể được xây dựng lại sau thảm họa.



Một ví dụ về một trang web nóng sẽ là một trung tâm hoạt động thứ cấp có đầy đủ nhân viên và tiếp xúc thường xuyên với mạng lưới các trung tâm chính trong điều kiện bình thường. Một trang ấm áp có thể là một trung tâm dịch vụ

khách hàng có thể được chuyển đổi một cách nhanh chóng để sử dụng như một cơ sở bảo trì mạng, nếu cần thiết. Và một trang web lạnh có thể là không có gì nhiều hơn một nhà kho cho thuê với sẵn điện và mạng lưới các kết nối, nơi thiết bị quan trọng có thể được di chuyển và cài đặt trong trường hợp thiên tai.

Kế hoạch dự phòng IT

Một kế hoạch dự phòng CNTT là một thành phần của BCP chỉ định thủ tục dự IT thay thế mà bạn có thể chuyển sang khi bạn đang phải đối mặt với một cuộc tấn công hoặc sự gián đoạn của dịch vụ dẫn đến một thảm họa cho một tổ chức. Các biện pháp tạm thời có thể bao gồm các hoạt động ra khỏi một trang web thay thế, sử dụng thiết bị thay thế hoặc các hệ thống, và di chuyển các hệ thống chính.

Orient Key Personnel

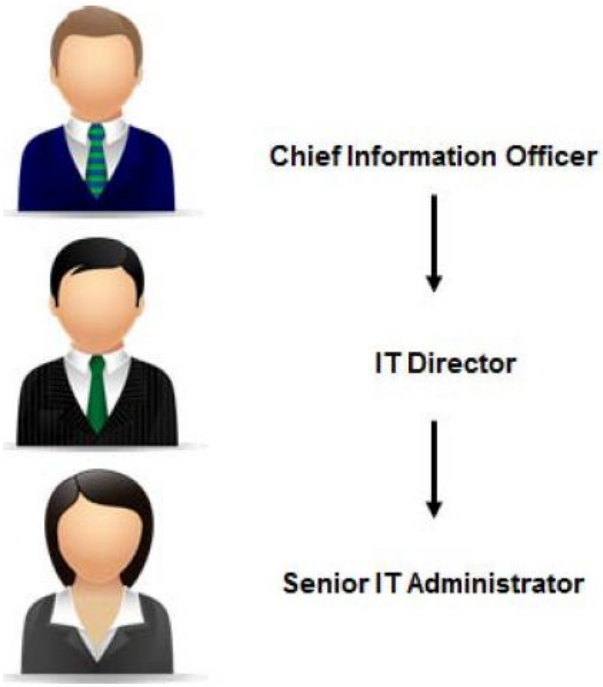
Review Checklist

Train and Prepare

Kế hoạch dự phòng.

Kế Hoạch kế nhiệm

Một kế hoạch kế nhiệm đảm bảo rằng tất cả các nhân viên kinh doanh chủ chốt có một hoặc nhiều bản sao lưu được những người có thể thực hiện các chức năng quan trọng khi cần thiết. Một kế hoạch tiếp nhận dạng cá nhân, những người mà họ có thể thay thế, mà chức năng của chúng, và làm thế nào họ cần phải được đào tạo.



Hình 8-9: Lập kế hoạch kế nhiệm.

Các phương pháp kiểm tra Business Continuity

Bạn có thể sử dụng phương pháp khác nhau để kiểm tra một BCP, cũng như đội ngũ nhân viên làm quen với nhiệm vụ và trách nhiệm của mình.

Kế hoạch khôi phục thảm họa

Bạn biết rằng tổ chức của bạn cần có một kế hoạch kinh doanh liên tục cho tổng thể để các hoạt động kinh doanh có thể tiếp tục với rất ít hoặc không có sự gián đoạn trong một thảm họa. Là một phần của kế hoạch đó, là một chuyên gia bảo mật, bạn cần phải hỏi câu hỏi kỹ thuật cụ thể như, "những gì về các dữ liệu nhạy cảm đã bị mất hoặc bị hư hại trong cuộc tấn công?" Trong chủ đề này, bạn sẽ phát triển một kế hoạch cho thảm họa phục hồi.

Lập kế hoạch khôi phục thảm họa là rất quan trọng cho sự an toàn của hệ thống kinh doanh lớn. Để cho các tổ chức để đảm bảo sự an toàn của hệ thống thông tin, họ phải chủ động và phát triển một DRP hiệu quả để đảm bảo rằng nếu có bao giờ một cuộc tấn công hệ thống lớn hoặc sự kiện môi trường, thông tin nhạy cảm có thể được bảo vệ hoặc, tồi tệ nhất, phục hồi.

DRPs

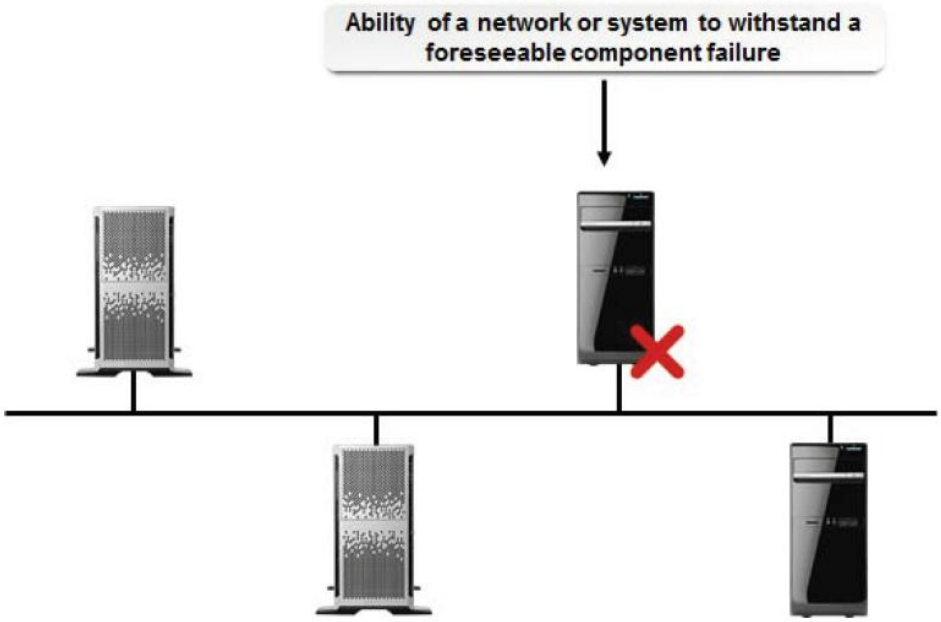
Một kế hoạch khôi phục thảm họa (DRP) là một kế hoạch chuẩn bị cho một tổ chức để phản ứng một cách thích hợp nếu là điều tồi tệ nhất xảy ra, có thể là tự nhiên hoặc một thảm họa do con người làm ra, và cung cấp các phương tiện để phục hồi từ thảm họa như vậy. DRPs giúp các tổ chức để phục hồi từ một tai nạn mà không mất nhiều thời gian và tiền bạc. Mối quan tâm quan trọng nhất của kế hoạch này, tuy nhiên, là sự an toàn của nhân viên. Một DRP có thể bao gồm:

- Một danh sách và thông tin liên lạc của các cá nhân chịu trách nhiệm cho việc phục hồi.
- Một hàng tồn kho của các phần cứng và phần mềm.
- Một kỷ lục kinh doanh quan trọng và thông tin khách hàng rằng bạn sẽ yêu cầu tiếp tục kinh doanh.
- Một kỷ lục của qui trình hướng dẫn và thông tin quan trọng khác như các BCP và các kế hoạch CNTT.
- Thông số kỹ thuật cho các trang web khác.

Chịu lỗi

Chịu lỗi là khả năng của một mạng lưới hoặc hệ thống để chịu được một thành phần thất bại có thể dự đoán và tiếp tục cung cấp một mức độ chấp nhận của dịch vụ. Có một số các nhóm biện pháp khả năng chịu lỗi, bao gồm cả những người bảo vệ nguồn điện, các ổ đĩa và lưu trữ dữ liệu, và các thành phần mạng.

Lỗi hệ thống khoan dung thường sử dụng một số loại trùng lặp hoặc dư thừa của nguồn lực để duy trì chức năng nếu một thành phần bị hư hỏng hoặc bị *lỗi.*



Các biện pháp dự phòng

Thời gian để thất bại (MTTF) có nghĩa là đánh giá dự đoán khoảng thời gian mà một thiết bị hoặc phần dự kiến sẽ đi vào hoạt động. MTTF thường được sử dụng để đánh giá độ tin cậy của các thiết bị và linh kiện mà không được sửa chữa.

Thời gian giữa thất bại có nghĩa là (MTBF) là đánh giá trên một thiết bị hoặc thiết bị dự báo thời gian dự kiến giữa thất bại. Dựa trên MTTF và / hoặc MTBF của một hệ thống, bạn cần xem xét kế hoạch cho đảm bảo dự phòng cần thiết

High Availability

Tính sẵn sàng cao là một đánh giá có biểu hiện như thế nào chặt chẽ hệ thống tiếp cận mục tiêu cung cấp dữ liệu sẵn có 100 phần trăm thời gian trong khi duy trì một mức độ cao về hiệu suất hệ thống. Hệ thống Highavailability thường được đánh giá là một tỷ lệ phần trăm cho thấy tỷ lệ thời gian hoạt động dự kiến tổng thời gian. Một số phương pháp được sử dụng trong việc đạt được này bao gồm clustering, cân bằng tải, và các biện pháp dự phòng.

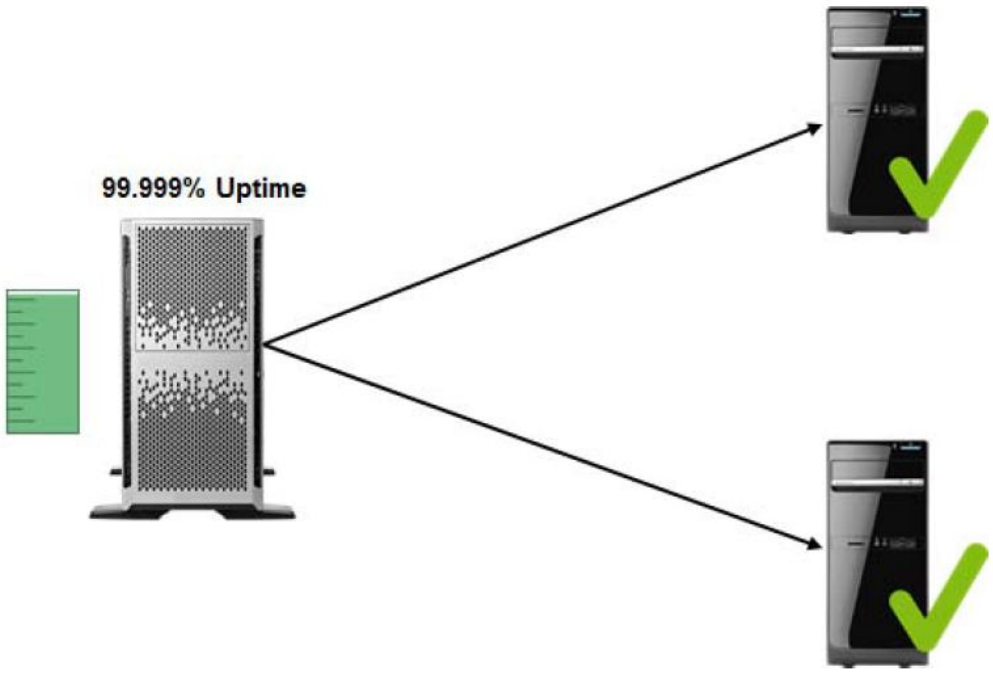


Figure 8-12: High availability.

Đánh giá thời gian hoạt động của 99,999% hay "năm nines" là một mức rất cao sẵn có, kết quả là ít hơn sáu phút của thời gian chết mỗi năm. "Sáu nines," hoặc 99,9999% thời gian hoạt động, kết quả trong khoảng 30 giây của thời gian chết mỗi năm, nhưng đi kèm với sự gia tăng tỷ lệ thuận liên quan trong chi phí.

DRP Testing and Maintenance

Mỗi DRP phải được kiểm tra định kỳ như một phần của việc thực hiện và quá trình phát triển DRP của bạn nên bao gồm một giai đoạn đánh giá để đảm bảo tính hiệu quả của nó. Bạn có thể sử dụng phương pháp thử nghiệm và kỹ thuật đánh giá tương tự như những người sử dụng để đánh giá một BCP, hoặc bạn có thể sử dụng các bài tập lập kế hoạch khẩn cấp như những phát triển bởi Cơ quan Quản lý Khẩn cấp Liên bang Mỹ (FEMA). FEMA công nhận và khuyến cáo về một số dạng bài tập mà bạn có thể sử dụng để đánh giá DRPs.

Hướng dẫn lập kế hoạch cho Disaster Recovery

Để có kế hoạch khắc phục thảm họa, bạn phải đánh giá đúng tình trạng hiện tại của tổ chức bạn sẵn sàng, và bạn phải biết khi nào và làm thế nào để cải thiện bất kỳ hạn chế của chiến lược hiện nay.

Giữ các hướng dẫn sau đây trong tâm trí:

- Nếu tổ chức của bạn đã không được thử nghiệm các BCP hoặc DRP gần đây, làm như vậy. Tiến hành một số kịch bản ẩn mà sử dụng các nguồn lực chỉ sao lưu.
- Nếu bạn đang tạo ra hoặc cải thiện các BCP và / hoặc DRP, nghiên cứu bất kỳ mẫu có sẵn mà có thể giúp hướng dẫn bạn. Các trang web như www.disasterrecoveryforum.com hoặc www.disasterrecoveryworld.com là những nơi tốt để bắt đầu.
- Đảm bảo rằng có những biện pháp dự phòng tại chỗ cho các máy chủ, nguồn điện, và ISP của bạn.
- Xác minh rằng các công ty có quyền truy cập vào phần cứng và thiết bị ngoại vi phụ tùng dùng cho trường hợp khẩn cấp, và rằng các thiết bị này có đủ an toàn để tiến hành kinh doanh với.
- Xem lại bất kỳ thỏa thuận mức độ dịch vụ (SLAs) mà là ở vị trí để bạn có một ý tưởng về những gì cấu downtime chấp nhận được.
- Tạo một dòng của truyền thông mà không làm cho việc sử dụng các nguồn lực của công ty, vì vậy nó không phá vỡ nên công ty mất điện sau giờ. Làm tương tự trong trường hợp các thành phố hoặc khu vực điện là xuống.
- Xác định và tài liệu tất cả các điểm duy nhất của thất bại, cũng như bất cứ up-to-date các biện pháp dự phòng.
- Hãy chắc chắn rằng dự phòng lưu trữ của công ty là an toàn.
- Hãy chắc chắn rằng bạn bao gồm DRP quy định đối với các bài kiểm tra thường xuyên của kế hoạch. Bạn có thể muốn sắp xếp một "khoan lửa", nơi mà một ngày, tất cả các nhà quản lý được chuyển đến một vị trí ngoại vi, không báo trước. Điều này giúp cho mô phỏng một thảm họa hoặc tình trạng khẩn cấp, mà không phải lúc nào cũng có thể cảnh báo dư dật.
- Nhân viên phải được đào tạo để hiểu được tầm quan trọng của DRP.

Thực thi DRPs và các thủ tục

Mặc dù bạn có biết làm thế nào quan trọng đó là tạo ra và thử nghiệm một DRP, các thử nghiệm thực sự của một kế hoạch được đưa vào hiệu lực trong một tình huống thảm họa thực sự. Trong chủ đề này, bạn sẽ thực hiện một DRP và thủ tục của nó.

Việc sử dụng một DRP tốt là gì nếu nó không phải là tốt thực thi? Biết những người liên hệ và biết làm thế nào để thực hiện một DRP theo cách tốt nhất có thể sẽ giúp có được kinh doanh trở lại và chạy trong thời gian không và tránh tất cả các thiệt hại không cần thiết cho tổ chức.

Tiến trình khôi phục thảm họa

Quá trình phục hồi thảm họa bao gồm một số bước để tiếp tục hoạt động kinh doanh đúng cách sau khi một sự kiện gây rối.

Thông báo cho các bên liên quan

Bắt đầu hoạt động khẩn cấp

Đánh giá thiệt hại

Đánh giá cơ sở tiện ích

Bắt đầu quá trình phục hồi

Nhóm khôi phục

Đội ngũ phục hồi là một nhóm các cá nhân được chỉ định người thực hiện thủ tục phục hồi và phục hồi hoạt động kiểm soát trong các sự kiện của một sự gián đoạn nội bộ hay bên ngoài quy trình kinh doanh quan trọng. Đội ngũ phục hồi ngay lập tức phản ứng trong trường hợp khẩn cấp và khôi phục các quá trình kinh doanh quan trọng để hoạt động bình thường của họ, tại trang web từ xa hoặc phục hồi, một khi dịch vụ chính và các hệ thống thông tin đang trở lại trực tuyến. Thành viên trong nhóm có thể bao gồm các hệ thống quản lý, quản trị hệ thống, quản trị an ninh, các chuyên gia cơ sở, các chuyên gia truyền thông, đội ngũ nhân lực, và đại diện pháp lý.

Hình 8-13: Các đội khôi phục cung cấp đáp ứng ngay lập tức.

Phục hồi an toàn

Các BCP hoặc DRP phải bao gồm các điều khoản về an toàn khôi phục dữ liệu, hệ thống và tài nguyên nhạy cảm khác. Điều này có nghĩa là chỉ định một quản trị tin cậy để giám sát việc thu hồi, cũng như ghi lại các bước và các thông tin cần thiết để khôi phục lại các quy trình, hệ thống và dữ liệu cần thiết để phục hồi từ thảm họa, và hướng dẫn cho các hoạt động tiếp tục vào lúc hoặc trang web chính hoặc một người thay thế site. Quá trình phục hồi an toàn nên được xem xét và kiểm tra một cách thường xuyên.

Hình 8-14: Thủ tục phục hồi an toàn.

Các loại sao lưu và phục hồi kế hoạch

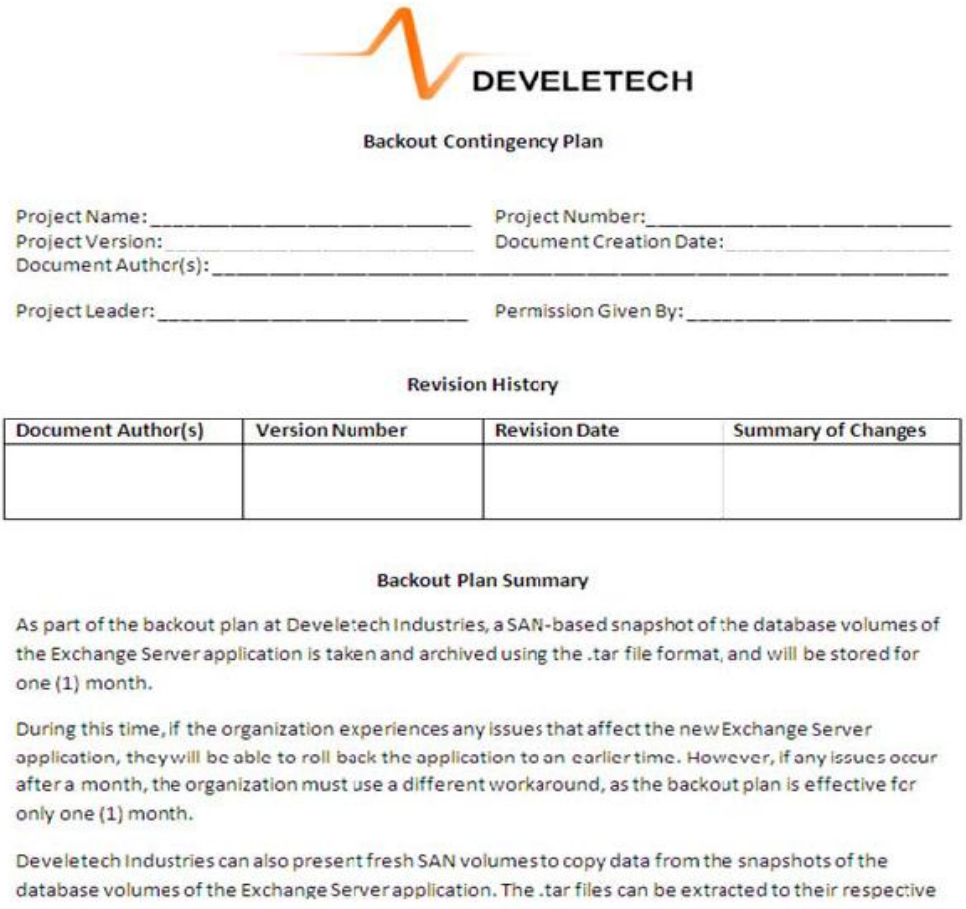
Quá trình phục hồi dữ liệu từ một bản sao lưu khác nhau tùy thuộc vào loại sao lưu đã được bao gồm trong kế hoạch dự phòng ban đầu. Có ba loại chính của các bản sao lưu.

- Backup toàn bộ
- Backup khác biệt

- Incremental backup

Backout Kế Hoạch Dự Phòng

Một kế hoạch backout ngờ là một kế hoạch tài liệu bao gồm các thủ tục và quy trình cụ thể được áp dụng trong trường hợp có sự thay đổi hoặc sửa đổi được thực hiện cho một hệ thống phải được hoàn tác. Kế hoạch này có thể bao gồm các cá nhân quan trọng, một danh sách các hệ thống, khung thời gian backout, và các bước cụ thể cần thiết để hoàn toàn thay đổi. Một phần của kế hoạch này cũng có thể bao gồm một kế hoạch backup có thể được triển khai như là một phần của quy trình và thủ tục backout.



DEVELETECH

Backout Contingency Plan

Project Name: _____ Project Number: _____
Project Version: _____ Document Creation Date: _____
Document Author(s): _____

Project Leader: _____ Permission Given By: _____

Revision History

Document Author(s)	Version Number	Revision Date	Summary of Changes

Backout Plan Summary

As part of the backout plan at Develetech Industries, a SAN-based snapshot of the database volumes of the Exchange Server application is taken and archived using the .tar file format, and will be stored for one (1) month.

During this time, if the organization experiences any issues that affect the new Exchange Server application, they will be able to roll back the application to an earlier time. However, if any issues occur after a month, the organization must use a different workaround, as the backout plan is effective for only one (1) month.

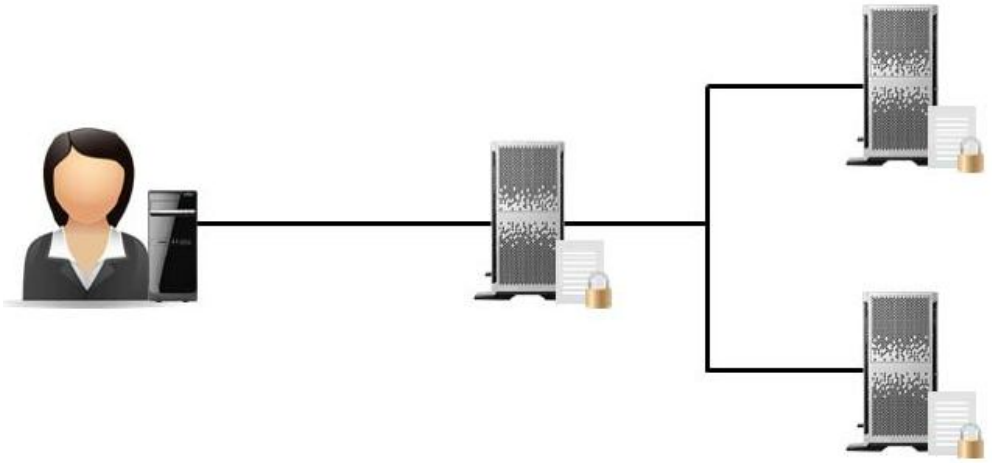
Develetech Industries can also present fresh SAN volumes to copy data from the snapshots of the database volumes of the Exchange Server application. The .tar files can be extracted to their respective

Hình 8-15: Một kế hoạch backout phòng.

Sao lưu an toàn

Sao lưu dữ liệu nhạy cảm hoặc quan trọng chỉ là một phần của giải pháp, như sao lưu đó cũng cần phải được an toàn. Lưu trữ bản sao của thông tin nhạy cảm hoặc quan trọng là một thực tế an ninh hợp lý, và không nên chỉ đơn giản

được giới hạn trong một đĩa cứng thứ cấp, một Compact Disc-Recordable (CD-R), hay một kho lưu trữ băng. Một bản sao lưu có thể được coi là an toàn nhất khi đang ngoại tuyến và ngoại vi, và được lưu trữ trong một môi trường được thể chất bị khóa và bảo vệ khỏi sự xâm nhập từ môi trường như lửa hoặc nước.



Hình 8-16: Secure backups.

Sao lưu Địa điểm lưu trữ

Các băng từ hoặc các phương tiện vật chất khác được sử dụng để tạo ra các bản sao lưu dữ liệu phải được lưu trữ an toàn, nhưng phải còn có thể truy cập trong trường hợp dữ liệu là cần thiết. Nhiều tổ chức sử dụng cả hai chỗ và ngoại vi lưu trữ dự phòng. Các vị trí lưu trữ tại chỗ là cho các tập gần đây nhất của các sao lưu, để họ có thể được truy cập một cách nhanh chóng nếu một phục hồi dữ liệu là cần thiết trong quá trình hoạt động bình thường. Các vị trí ngoại vi là một, cơ sở lưu trữ thiên tai chống an toàn nơi tổ chức giữ hoặc là một trùng lặp hoặc một backup cũ thiết lập để bảo vệ nó chống lại bất kỳ thiệt hại gây ra bởi điều kiện thiên tai tại các trang web chính.

Hình 8-17: Địa điểm lưu trữ Backup.

Hướng dẫn Thực hiện DRPs và Thủ tục

Để thực hiện DRPs và thủ tục, bạn cần phải đảm bảo rằng các DRPs được đưa ra và có thể dễ dàng thực hiện trong trường hợp có thảm họa. Giữ các hướng dẫn sau đây trong tâm trí:

- Các tổ chức cần phải xác định đội nào sẽ xử lý các tình huống thảm họa, bao gồm cả người quản lý sự cố.
- Mỗi thành viên trong nhóm phải khắc phục thảm họa đã đặt ra rõ vai trò và trách nhiệm và phải được dễ dàng tiếp cận với các nhân viên khác.
- Nhân viên phải được nhận thức của các thành viên của nhóm nghiên cứu khắc phục thảm họa và phải biết họ cần phải liên hệ trong trường hợp có thảm họa.
- Đội ngũ phục thảm họa phải đề ra một kế hoạch dự phòng cho các sự kiện đó sẽ đảm bảo rằng sự liên tục của doanh nghiệp không bị ảnh hưởng như là một hậu quả của thiên tai.
- Thông báo cho các bên liên quan theo quy định tại DRP của bạn
- Lăn ra các dịch vụ khẩn cấp, chẳng hạn như một trang web khác, dưới sự điều khiển của người quản lý sự cố.
- Các thiệt hại cho các trang web chính cần được đánh giá, và đội phục hồi nên được đưa vào để sửa chữa bất kỳ thiệt hại vật chất và đánh giá mức độ mà các trang web chính có thể được phục hồi.

- Một phục hồi của các sao lưu nên được thực hiện của tất cả các tập tin đã bị xâm nhập hoặc bị xóa.
- Các quyết định phải được thực hiện để mua hoặc thay thế các thành phần hệ thống còn thiếu.
- Một khi quá trình khôi phục hoàn tất, tài liệu các các bước thực hiện và lưu một bản báo cáo được sử dụng trong trường hợp của một quá trình phục hồi.