5 bước để kiểm soát chặt chẽ mạng và người sử dụng

12/16/2004 10:48:00 AM

Với các mối đe dọa đến an ninh mạng ngày càng gia tăng, chẳng có gì đáng ngạc nhiên khi các công ty đang xem xét lại các chiến lược bảo vệ để kiểm soát người sử dụng và bảo vệ các mạng nội bộ và các dữ liệu quan trọng của mình.

Các chuyên gia an ninh mạng đang ở vào một tình thế rất khó xử, bị kẹt giữa sự cần thiết phải hỗ trợ quá trình sản suất của người sử dụng và sự linh hoạt trong một tổ chức, trong khi vẫn phải đảm bảo an ninh cho những truy nhập vào các dữ liệu quan trọng. Vì ranh giới phân cách đã bị loại bỏ, họ đang phải đối mặt với những đợt tấn công không ngừng. Điều này làm gia tăng sự phức tạp và chí phí, cũng như làm gia tăng áp lực về mặt quy định. Rõ ràng rằng chỉ sử dụng những chiến lược vành đai truyền thống không còn hiệu quả nữa đối với các doanh nghiệp được kết nối qua lại ở mức độ cao như hiện nay.

Các tổ chức đang cố gắng hết sức để giải quyết vấn đề bằng các công cụ hiện có trong tay, triển khai các lớp an ninh vành đai trên các mạng nội bộ để giám sát người sử dụng và kiểm soát truy nhập. Trong khi biện pháp này đã làm giảm một phần nguy cơ thì chi phí lại rất cao vì những công nghệ này chưa từng được thiết kế để bảo vệ các mạng nội bộ doanh nghiệp không đồng nhất và phức tạp hơn.

Lợi thế lớn nhất so với các tin tặc

Việc bảo vệ mạng nội bộ của bạn được dựa trên việc xác thực một lần, các mật khẩu và/hoặc các thẻ, giống như xuất trình giấy chứng minh thư của bạn tại cửa ra vào, nhưng sau đó là đi đến bất cứ nơi nào bạn muốn trong một tòa nhà đã được "bảo vệ".

Trong môi trường được quy định một cách chặt chẽ như hiện nay, việc xác thực một lần là chưa đủ để bảo vệ hệ thống của bạn khỏi những kẻ xâm nhập từ bên ngoài, bạn cũng phải kiểm soát và giám sát cả người dùng ở bên trong và có thể kiểm tra được họ là ai và họ đang làm gì. Trong thực tế, an ninh mạng phải phản ánh tình hình an ninh vật lý bằng cách gắn một "biển hiệu" tại cửa ra vào với sự bảo đảm về an ninh tại các khu vực chỉ định. Cuối cùng, việc biết được ai nên ở trên mạng của bạn là một lợi thế lớn nhất của bạn so với các tin tặc và những tên trộm nhân dạng.

Đối với hầu hết các tổ chức doanh nghiệp, việc bảo vệ bên trong bao gồm cả việc triển khai một phương pháp đa lớp. Phương pháp này bao gồm một sự kết hợp của các bức tường lửa, các hệ thống phát hiện xâm nhập, kiểm tra gói sâu, kiểm soát truy nhập, phần mềm chống vi rút và quy trình vá lỗ hổng nghiêm ngặt. Nhưng vì các nguy cơ và áp lực về những quy định ngày càng gia tăng, các chi phí và mức độ phức tạp của việc duy trì những lớp này cũng tăng theo.

Chúng ta bắt đầu được thấy những phương pháp dựa trên nhân dạng, mang tính đổi mới được xây dựng để nhằm mục đích xử lý nhu cầu an ninh mạng nội bộ. Những nhu cầu này có thể được mở rộng mà không cần thêm các yêu cầu về quản lý hay chí phí phụ trội. Các chuyên gia an ninh phải sẵn sàng đánh giá hiệu quả của chiến lược an ninh doanh nghiệp nội bộ hiện tại của họ và các giải pháp sáng tạo kết hợp để đối mặt với những thách thức của một mạng và vành đai phân cách luôn luôn thay đổi.

5 bước để giành quyền kiểm soát

Những gợi ý mang tính tiên phong thực hiện dưới đây sẽ giúp bạn giành được quyền kiểm soát người sử dụng của bạn cũng như cải thiện tình hình an ninh xung quanh những dữ liệu quan trọng của cơ quan bạn.

Hãy nhớ rằng an ninh nội bộ rất khác so với an ninh vành đai

Mô hình mối đe dọa đối với an ninh nội bộ khác so với mô hình của an ninh vành đai. An ninh vành đai bảo vệ mạng của bạn khỏi những kẻ tấn công trên Internet được trang bị với những công cụ khai thác của các dịch vụ Internet phổ biến như HTTP và SMTP. Mô hình an ninh nội bộ phải đối phó với chính những kẻ xấu ở trong công ty. Các mạng nội bộ bây giờ nhanh hơn, phức tạp và biến động hơn. Thêm vào đó, lối truy nhập vào mạng nội bộ của bạn của một người ở bên trong mạng, đơn giản chỉ bằng cách cắm vào một giắc Ethernet, còn nguy hiểm hơn nhiều lối truy nhập bằng các script của một tin tặc tinh vi.

Bạn không còn có thể giả định rằng những người bên trong mạng nội bộ là "tin cậy" bởi vì nhóm người này thường bao gồm nhiều thành phần từ các đối tác kinh doanh, các nhà đầu tư, các nhà tư vấn đến các khách hàng. Cho dù bạn tin tưởng mọi người trên mạng nội bộ của mình, nguy cơ vẫn còn vì hầu hết các lỗ hổng xuất phát từ sự bất cẩn hơn là sự sử dụng sai có chủ định. Do vậy, chúng ta phải đối mặt với nhiều thách thức xung quanh việc kiểm soát sự truy nhập của người dùng và bảo vệ các dữ liệu mạng nội bộ.

Bảo vệ các tài nguyên quan trọng

Các báo cáo như Báo cáo về nguy cơ an ninh Internet định kỳ nửa năm 1 lần của công ty Symantec khẳng định rằng các công ty có giao dịch tài chính trực tuyến, chẳng hạn như các ngân hàng và các dịch vụ thanh toán, là những mục tiêu chính của các vụ tấn công trên mạng. Báo cáo hàng năm của SANS về 20 lỗ hổng an ninh Internet hàng đầu cũng cho thấy một nguy cơ cao liên quan đến các máy chủ Web và các hệ điều hành phổ biến. Những thông tin này cần phải được các doanh nghiệp sử dụng để ưu tiên một cách hợp lý các dự án cho các tài nguyên an ninh và công nghệ thông tin.

Vậy bạn đã xếp hạng các hệ thống nội bộ của bạn theo mức độ quan trọng đối với công ty hay chưa? Bạn nghĩ tới các máy chủ hay ứng dụng nào mà dữ liệu trên đó chỉ cần cho một bộ phận nhỏ nhân viên? Có một tài sản nào (ứng dụng hay cơ sở dữ liệu hay máy chủ) ở "bên trong" quan trọng đến nỗi mà bạn nghĩ rằng sẽ gắn thêm yêu cầu xác nhận khi truy nhập vào đó. Hoặc là bạn đã xem xét đến việc sử dụng các tường lửa hoặc IDS để bao quanh nó chưa? Dành ưu tiên, nhưng bạn hãy nhớ rằng những thiết bị này hoạt động với các địa chỉ IP vốn có thể bị giả mạo, chiếm đoạt hoặc ăn cắp.

Trên một mạng với 30.000 người sử dụng, sẽ là không thực tế khi hy vọng mọi máy chủ có thể luôn được khóa và vá khi có lỗ hổng. Xếp loại nguy cơ an ninh của bạn và thực hiện một phân tích chi phí-lợi nhuận cùng với nhiều phương án giải quyết. Phân loại những tài sản mới dựa trên giá trị đối với doanh nghiệp và ảnh hưởng về mặt tài chính của thời gian bị ngừng hoạt động. Có thể sẽ mất một tháng để tìm, ghi thành danh mục, phân loại và đánh giá các lỗ hổng cho mỗi máy chủ web trên mạng, nhưng thời gian đầu tư vào đó là đúng đắn và thiết thực.

Bây giờ bạn có một danh sách các máy chủ web, được xếp hạng ưu tiên theo nguy cơ và giá trị tài sản, đánh giá xem những máy chủ nào là được bảo vệ ít nhất và xử lý những máy chủ đó trước. Ví dụ, các máy chủ web ở DMZ cần được quan tâm ngay lập tức hơn là những máy chủ ít truy nhập được vào hơn bởi vì chúng nằm sâu hơn bên trong mạng của bạn và được bảo vệ bởi nhiều lớp an ninh hơn. Sau cùng, xác định bất cứ máy chủ web nào có một giá trị tài sản cao nhưng không thể được vá bởi vì tính tương thích hay vì các vấn đề khác. Những máy chủ này phải được di chuyển tới một khu vực tin cậy của

mạng nội bộ của bạn với những rào cản cao cấp giữa chúng và phần còn lại của thế giới (những vành đai ảo).

Tắt các dịch vụ mạng không sử dụng

Điều này dường như là hiển nhiên, mặc dù nó vẫn tiếp tục là một lỗ hổng để tin tặc khai thác. Hầu hết các hệ thống và phần mềm có rất nhiều dịch vụ và cổng mở để làm cho quá trình triển khai và sử dụng trở nên dễ dàng hơn. Các dịch vụ truy nhập từ xa thường được bật lên theo ngầm định cho cả hai hệ thống Windows và Unix. Việc chia sẻ tập tin và gọi thủ tục từ xa (RPC) không được bảo vệ chỉ là hai ví dụ trong số các dịch vụ có nhiều khả năng bị tấn công.

Kiểm tra các máy chủ và máy tính trung tâm hiện có của bạn một cách thường xuyên để rà soát các dịch vụ này và khóa chúng lại khi chúng không chạy. Hầu hết các công ty đều có một chuẩn riêng cho các hệ thống người dùng. Bạn hãy chắc chắn rằng chuẩn của bạn loại trừ tất cả các dịch vụ truy nhập từ xa phổ biến đối với hệ điều hành đang sử dụng. Hãy nhớ rằng việc chặn các dịch vụ phổ biến này ở bức tường lửa chỉ bảo vệ chúng khỏi những truy nhập từ bên ngoài. Bạn vẫn phải quan tâm đến những máy tính xách tay lưu động và các cuộc tấn công từ bên trong.

Tạo ra các vành đai ảo

Như bạn đã biết, vành đai phân cách đã bị loại bỏ. Vậy bạn nên làm gì? Hãy bắt đầu bằng việc đánh giá xem mạng của bạn được sử dụng như thế nào và xây dựng các vành đai ảo xung quanh các đơn vị kinh doanh. Các máy chủ sẽ vẫn dễ bị tấn công chừng nào con người còn vận hành chúng. Thay vì tạo ra những mục tiêu không thực tế như "không có máy chủ nào bị làm hại", một mục tiêu khả thi hơn là không có một máy chủ nào có thể cho phép một kẻ xâm nhập truy nhập hoàn toàn vào mạng nếu nó bị làm hại.

Nếu một máy tính của nhân viên marketing bị làm hại, kẻ tấn công phải không truy nhập được vào bộ phận nghiên cứu & phát triển (R&D) của công ty. Vì vậy bạn hãy thực hiện việc kiểm soát truy nhập giữa bộ phận R&D và marketing. Chúng ta đã biết cách xây dựng các vành đai giữa Internet và mạng nội bộ. Đã đến lúc cần phải thiết lập các vành đai giữa những nhóm người sử dụng khác nhau trong mạng doanh nghiệp .

Biết được người sử dụng của bạn là ai bằng cách thực thi việc kiểm tra nhân dạng

Bước tiếp theo là xác định người sử dụng của bạn là ai, những tài nguyên nào họ được phép truy nhập và sau đó thực thi những chính sách kiểm soát truy nhập đó cho các ứng dụng và máy chủ nội bộ. Thế mạnh chủ yếu của bạn để bảo vệ mạng nội bộ của bạn ở mức này là bạn biết là ai nên ở đó và vị trí của họ. ở lớp bảo vệ này, nhận dạng bằng một địa chỉ IP là phương án có thể chấp nhận được. Giải pháp này phải hỗ trợ việc xác định nhân dạng đó để lớp bảo vệ nội bộ cuối cùng có thể cấp cho người dùng đã biết lối truy nhập với mức độ chi tiết phù hợp.

Việc xác thực là rất tốt và cần thiết, nhưng bạn hãy luôn nhớ rằng việc này chỉ có hiệu lực một lần, vào lúc đăng nhập. Bạn cũng cần phải nhớ rằng các bức tường lửa nội bộ và IDS không thể kiểm soát nhân dạng và hoạt động trên các địa chỉ IP là những thứ thường xuyên thay đổi và rất dễ bị giả mạo bởi tin tặc. Bằng việc gắn một "dấu hiệu nhận dạng" khi truy nhập vào một mạng, các tổ chức có thể giám sát một cách hiệu quả hạn chế truy nhập và cấm truy nhập đối với những người không được phép.

Thế hệ thứ hai của Quản lý nhân dạng sẽ giúp chúng ta đi theo hướng này. Ban đầu, Quản lý nhân dạng tập trung vào tích hợp việc xác thực, kiểm soát truy nhập và quản lý mật khẩu. Nhưng khi các tổ chức triển khai Quản lý nhân dạng, họ bắt đầu nhận ra rằng có một khe hở giữa ứng dụng và lớp mạng và chỉ

bằng cách tổ chức tính toán xung quanh nhân dạng và quản lý nó bằng nhân dạng thì vấn đề truy nhập mới có thể được giải quyết.

Theo tạp chí BCVT & CNTT

In trang này | Đóng cửa sổ