

MƯỜI MẸO GIÚP BẠN ĐẠT HIỆU QUẢ HƠN TRONG KHAI THÁC MẠNG

Mẹo th

Mẹo thứ nhất: Hoà hợp với nhà cung cấp dịch vụ mạng (IPS)

Rất nhiều người có tâm lý “cài đặt rồi quên” các thiết lập hệ thống. Điều đó thật nguy hiểm, tạo lỗ hổng cho những kẻ khai thác liên tục rình mò xung quanh mạng, chờ cơ hội tấn công.

Phương thức khai thác điểm yếu, lỗ hổng bảo mật thay đổi nhanh đến chóng mặt, khiến phần mềm tường lửa, các bản vá lỗi hay hàng rào ngăn chặn của nhà sản xuất khó có thể đáp ứng kịp thời.

Các nhà quản lý mạng cần hiểu hoạt động khai thác diễn ra như thế nào và hãng cung cấp dịch vụ Internet (ISP) dò tìm chúng ra sao. Đồng thời cũng phải nâng cấp thường xuyên chương trình bảo vệ, cập nhật phiên bản mới nhất. Tất nhiên không có phần mềm ngăn chặn nào vạn năng, nhưng liên tục sử dụng các bản mới nhất sẽ giúp tăng cường an toàn cho mạng ở mức tối đa.

Mẹo thứ hai: Bán các hình thức bảo mật từ lợi ích của chính nó

Bán lợi ích bảo mật cho các nhà đầu tư công nghệ là cách mà Mandy Andress, chủ tịch của Technologies ArcSec đề xuất. Thay vì nói các virus nguy hiểm như thế nào, sao bạn không đưa ra phương thức đem lại lợi nhuận cho các công ty với dịch vụ danh tiếng, như hàng rào bảo vệ chống spam chẳng hạn. Hãy phác hoạ cho người dùng hiểu hiệu quả cụ thể tăng lên bao nhiêu lần khi thêm một tầng khác cho điều khiển chống spam và lợi ích của họ sẽ đạt được là gì.

Mẹo thứ ba: Truy cập mạng và máy để bàn tự động

Các dấu hiệu không dây có thể rất hữu ích cho điều khiển truy cập tự động máy tính để bàn, thường được chia sẻ bởi đa người dùng ở những nơi như các phòng kiểm tra thuốc, kho hàng, trung tâm tư vấn (call centre)...

Ví dụ, một nhóm các nhà vật lý bộ nhớ đã từng triển khai XyLoc MD của Ensure Technologies, sử dụng kỹ thuật tần số radio 900MHz để mã hoá ID nhân viên cho hoạt động thẩm định. Phương thức này giúp tiết kiệm thời gian cho nhân viên trong khi vẫn đảm bảo quyền truy cập mạng và thông tin nhạy cảm không bị xâm phạm bởi bất kỳ ai khác.

Mẹo thứ 4: Liên kết truy cập vật lý với chương trình ứng dụng doanh nghiệp

Các hệ thống truy cập cao tầng dựa trên địa chỉ IP với các server tiêu chuẩn công nghiệp, sử dụng mạng dữ liệu đã tồn tại đem lại hiệu quả tốt nhất chưa từng có từ trước đến nay. Thành công của dòng hệ thống này là nhờ các sản phẩm kiến trúc mở của chúng. Điểm nâng cao trong công nghệ quản lý server là ở chỗ, các hệ thống không chỉ được triển khai nhờ nhân viên mạng (tốt hơn chế độ bảo mật vật lý), mà còn có thể quản lý trung tâm hoá. Thêm vào đó, chúng còn tích hợp được với các chương trình ứng dụng ERP và các hệ thống điều khiển truy cập mạng.

Georgia Pacific, hãng sản xuất giấy với tài sản 20 tỷ đô la ở Atlanta (Mỹ), đã phát hành WebBrix, một sản phẩm của công nghệ quản lý tự động, là hệ thống truy cập cao tầng dựa trên địa chỉ IP, với phạm vi rộng lớn trên 400 khu vực. Các nhân viên IT đã sử dụng giao diện ứng dụng mở của WebBrix, viết ra một phần mềm tùy biến khác có tên Mysecurity, tích hợp hệ thống với SAP. Khi các nhân viên theo dõi dấu hiệu mạng nhằm có được quyền truy cập, họ cũng đồng thời gửi dữ liệu tới SAP và theo dõi những người tham dự.

Mẹo thứ 5: Giao phó lại cho một chuyên viên hệ điều hành

“Cấu hình các hệ điều hành có thể được ví như một thứ nghệ thuật ngầm”, Tom Henderson - chuyên gia nghiên cứu các vấn đề cơ bản của ExtremeLabs, hãng kiểm tra tính năng sản phẩm nhận định nói. Thiết lập kết nối sai có thể gây hậu quả nghiêm trọng. Như khi sử dụng tùy chọn di chuyển khối bộ nhớ lớn có thể tác động tới dung lượng sử dụng của Cache, khiến hệ điều hành phải ngừng hoạt động khác để xử lý. Nếu tùy chọn bộ nhớ/lưu trữ không được cân bằng hợp lý, máy tính có thể bị ngừng hoạt động. Bằng cách uỷ thác cho một chuyên gia có trình độ, làm chủ phần hướng dẫn của nhà sản xuất, server sẽ dễ dàng hoà hợp an toàn với thực thi tối ưu cho mọi ứng dụng. Các chuyên viên cũng nên làm chủ các tùy chọn thiết lập Web Server và BIOS.

Mẹo thứ 6: Sử dụng bộ nhớ server thông minh VMware

Nếu có điều kiện, bạn nên tăng cường dung lượng cho bộ nhớ trên các server vật lý Windows 2003 được ảo hoá. Từ đó, tăng tốc độ thực thi cho các máy ảo. Nếu tất cả các máy ảo trên một hộp vật lý cần cùng một mã nguồn nằm trong bộ nhớ giống nhau, như thư viện liên kết động (DLL), bạn có thể tải từng DLL vào bộ nhớ chính của server vật lý rồi chia sẻ DLL cho tất cả máy ảo. Chúng ta sẽ tăng ích lợi trong sử dụng bộ nhớ lớn bằng cách lưu trữ trên từng hộp vật lý thay vì theo mức sử dụng.

Mẹo thứ 7: Chuyển các ứng dụng sang lưới Linux

Nếu bạn có chương trình ứng dụng tính toán chuyên sâu cho máy vi tính lớn, đừng ngại chạy nó trên các lựa chọn rẻ tiền như máy tính lưới, vì các ứng dụng này được viết trên ngôn ngữ COBOL. Ứng dụng sẽ phải được thiết kế lại một chút cho phù hợp với nền tảng của phần cứng mới. Các hãng sản xuất có thể sẽ cần thêm trợ giúp, vì họ muốn liên kết trên nền công nghệ mới.

Mẹo thứ 8: Các liên kết WAN có thể gây suy biến VoIP QoS

Đây là vấn đề thực sự trên các khu vực có cơ sở hạ tầng công cộng đang lão hoá ở một số nước, Bruce Bartolf - giám đốc công nghệ của hãng kiến trúc Gensler ở San Francisco cho biết. Đã từng thực hiện lắp đặt hoàn chỉnh 7 trong tổng số 35 site VoIP, vị giám đốc này thấy rằng tỷ lệ lỗi xảy ra rất cao và có nhiều lỗi hoàn thiện trên nhiều liên kết. Để cung cấp dịch vụ điện thoại đảm bảo chất lượng cũng như đảm bảo thời gian thi công, bạn cần thiết kế với các đường không lỗi luân phiên trên mạng WAN. Cáp mạng có thể không cần tốt hơn. Metro Ethernet đáp ứng được yêu cầu bạn cần.

Mẹo thứ 9: Quản lý địa chỉ IP dễ dàng với một công cụ

Mặc dù chức năng của các công cụ có thể được thay thế bằng sản phẩm của nhà sản xuất, nhưng với những hoạt động quan trọng như quản lý địa chỉ IP, nếu không kiểm soát tốt, bạn đã tự mình phá hoại 5-9 phần. Bạn có thể sử dụng Infoblox, với khả năng quản lý vô số hoạt động, như nâng cấp phần mềm firmware TFTP (Trivial File Transfer Protocol). “Thay vì xử lý hệ thống file phân phối Microsoft, tôi tải server TFTP lên một server Microsoft, chạy DHCP cũng trên một server Microsoft, chạy SMS trên đầu và quản lý tất cả, khi đó tôi có một công cụ”, Bartolf của Gensler cho hay. Ông đã từng thực hiện hiệu quả phương thức này và khẳng định một cách đơn giản: “Tôi chỉ cần đặt nó vào, và nó làm việc”.

Mẹo thứ 10: Bỏ qua các hoạt động theo kiểu trực quan

Kinh nghiệm của một số công ty như VistaPrint ở Mỹ chỉ ra rằng, không nên triển khai các hoạt động giám sát trực quan. Hãng này từng dựa trên hoạt động giám sát từ xa để quản lý các trung tâm dữ liệu, trong đó một trung tâm ở Bermuda. Họ dùng công cụ tự phát triển để theo dõi mọi hoạt động, từ sử dụng CPU đến tương quan sự kiện. Đồ họa trực quan sự kiện có tốc độ dò tìm và phân tích chậm, thường phải mất từ 5 đến 7 phút cho một sự kiện. Trong khi các công cụ sử dụng màu sắc đơn giản (đỏ, vàng, xanh) chỉ mất từ 1 đến 2 phút.

Và đừng quên duy trì sử dụng các công cụ giám sát liên tục 24/7, đồng thời chạy các hoạt động kiểm tra. Lỗi phổ biến nhất thường xảy ra là không để chế độ mở cho các công cụ này cho đến khi có sự kiện xuất hiện.