CHỐNG VIRUS LÀ VẤN ĐỀ CỦA MỌI HỆ ĐIỀU HÀNH

Hãng bảo mật Sophos tin rằng quan điểm "các máy tính không chạy hệ điều hành Windows thì không cần bảo vệ chống virus" không còn đúng nữa. Đã bắt đầu xuất hiện một số virus tấn công các hệ điều hành khác như Macintosh, UNIX/Linux. T

Hãng bảo mật Sophos tin rằng quan điểm "các máy tính không chạy hệ điều hành Windows thì không cần bảo vệ chống virus" không còn đúng nữa. Đã bắt đầu xuất hiện một số virus tấn công các hệ điều hành khác như Macintosh, UNIX/Linux. Tuy nhiên, chúng mới chỉ chiếm khoảng 0,2% của toàn bộ các loại phần mềm nguy hiểm. Chúng ta sẽ phân tích về việc cần thiết phải bảo vệ các hệ điều hành khác khỏi virus, khám phá các mối đe dọa đối với các nền tảng đó, bởi vì chúng cũng có thể che giấu và phát tán các loại virus của Windows, nhất là trong bối cảnh hiện nay khi các hệ điều hành không phải Windows đang ngày càng được sử dụng phổ biến hơn. Các mối đe dọa hiện hữu Số lượng rất lớn các máy tính Windows đã làm chúng trở thành mục tiêu dễ dàng và dễ tìm cho các đối tượng lập trình các loại virus hay spam. Vì vậy mọi người thường chỉ tập trung vào việc chống virus máy tính cho môi trường Windows. Trong khi đó thì các nguy cơ bảo mật đang xuất hiện trên các hệ điều hành khác đôi khi lại không được quan tâm đúng mức. Theo thống kê của các trung tâm thí nghiệm hãng Sophos thì hiện nay họ đã xác định được tổng cộng là 120.000 virus, trong đó có 50 virus chuyên tấn công, lây lan trên Mac, và khoảng 100 Virus trên UNIX. Nói chung tất cả các lỗ hổng bảo mật trên tất cả các loại hệ thống khác nhau đều có thể bị khai thác. Ngày nay việc kết hợp giữa các đối tượng lập trình virus, gửi thư rác, và các Hacker ngày càng phổ biến hơn, chúng kết hợp với nhau để ăn cắp thông tin và tiền bạc từ các công việc kinh doanh tưởng như tin cậy hoàn toàn bằng các còn bài như phần mềm gián điệp, thư rác, thư lừa. Chính vì vậy mà các mối nguy hiểm lây lan trên môi trường không phải Windows không thể bị bỏ qua. OSX/Leap-A là một phần mềm nguy hiểm đầu tiên trên Mac OSX xuất hiện vào tháng 2/2006. Linux/Mare-A xuất hiện tháng 12/2005 và lây lan thông qua một lỗ hổng bảo mật của pHp script. Mối đe dọa giấu mặt đối với các máy tính Windows Rất dễ tìm thấy một máy chủ UNIX kết nối với một mạng lớn máy tính dùng Windows. Còn những mạng doanh nghiệp mà họ cho rằng không dùng Windows vẫn có một số máy Windows kết nối vào. Đây là một thực tế, cho dù đó là kết nối thật hay kết nối ảo thì việc bảo vệ toàn bộ các máy tính trong mạng là rất quan trọng. Về cơ bản một virus hay một sâu thực chất là một tệp tin. Nó có thể được chuyển đến các máy tính khác thông qua rất nhiều con đường như qua đĩa CD, DVD, ổ USB, thư điện tử, Internet, gửi tin nhắn. Mối đe dọa trong tương lai Ngoài Windows, có rất nhiều lý do để các hệ điều hành khác cũng sẽ trở thành mục tiêu nhắm đến của các đối tượng lập trình virus. Một điều chắc chắn là cả Mac và UNIX/Linux đang ngày càng trở nên phổ dụng hơn. Hãng Apple đã tăng trưởng doanh số tới 48% trong quý 3/2005 vừa qua, nhà phân tích thị trường Gartner thì nhận định là Linux sẽ đạt được tỷ lệ phát triển mạnh nhất trong vòng 5 năm tới. Để chống lại các thách thức về bảo mật thì chúng ta phải thực hiện giải pháp tiếp cận từ 2 phía, đó là tăng cường giáo dục cho người dùng về các kinh nghiệm và các giải pháp bảo vệ mạnh, tin cậy. Song song đó là việc triển khải một giải pháp chống virus cho tất cả các máy tính để đảm bảo cho việc an ninh thông tin và cảnh báo. Sophos là hãng chuyên về các giải pháp tích hợp quản lý các loại virus, sâu, thư rác cho các doanh nghiệp, ngân hàng, chính phủ, và trong giáo dục. Các sản phẩm của Sophos đã và đang bảo vệ hơn 35 triệu người dùng trên 150 quốc gia trên thế giới. L.Q.H