8 TÍNH NĂNG BẢO MẬT CỦA HỆ ĐIỀU HÀNH WINDOWS

Bạn đã

Bạn đã biết rõ về các tính năng bảo mật của hệ điều hành Windows chưa? Bài viết dưới đây sẽ giới thiệu với bạn đọc 8 tính năng bảo mật ưu việt của hệ điều hành Windows.

1. Dịch vụ xác thực của Microsoft

Hạ tầng khoá công cộng (PKI) là một yếu tố mang ý nghĩa sống còn khi thiết kế chính sách bảo mật tổng thể của các doanh nghiệp. Nền tảng của PKI là tạo và phân phối các chứng chỉ số mà sau đó có thể sử dụng để xác thực người dùng và các máy trong mạng. Một lựa chọn là sử dụng các dịch vụ của các tổ chức cung cấp dịch vụ xác thực chuyên nghiệp nhưng cách này có chi phí tương đối cao. Nếu máy chủ của bạn cài hệ điều hành Windows 2000 hoặc Windows Server 2003, bạn đã có riêng một "cơ quan cấp dịch vụ xác thực" với dịch vụ Microsoft Certificate Services để cấp chứng chỉ cho tất cả các máy tính và người dùng trong mạng của bạn. Bạn có thể cấu hình Microsoft Certificate Services để làm việc với chính sách nhóm của Active Directory để tự động triển khai cấp phát chứng chỉ số cho tất cả các máy được quản lý trong domain Active Directory.

2. Windows Firewall của Windows XP Service Pack 2

Giải pháp tường lửa đầu tiên của Microsoft cho máy tính cá nhân là Internet Connection Firewall (ICF). Mặc dù ICF hoạt động khá tốt, nó thiếu sự uyển chuyển và khả năng quản lý tập trung một cách hữu hiệu. Tất cả những vấn đề đó đã thay đổi với Windows Firewall. Windows Firewall cho phép bạn chặn cácư kết nối nguy hiểm tới các máy trạm cài hệ điều hành Windows hoặc cấu hình các biệt lệ theo ứng dụng hoặc số cổng. Bạn có thể tinh chỉnh các biệt lệ và cho phép một số kết nối từ một số địa chỉ mạng hay địa chỉ máy nhất định. Windows Firewall có thể được quản lý tập trung qua chính sách nhóm của Active Directory.

3. Microsofy Baseline Security Analyzer (MBSA)

MBSA là một công cụ miễn phí cho phép bạn quét các hệ thống máy trạm và máy chủ trên mạng của bạn để phát hiện các vấn đề nguy hiểm tiềm tàng trong cấu hình của các hệ thống này. Bạn có thể sử dụng giao diện theo dòng lệnh của công cụ để đặt lịch quét. Các thông tin sẽ được lưu trong một cơ sở dữ liệu với nội dung khá đầy đủ và rõ ràng.

4. VPN cho các đoạn mạng cần bảo mật cao

Phần lớn các nhà quản trị và chuyên gia bảo mật nghĩ rằng VPN chỉ đơn thuần là một giải pháp truy nhập từ xa. Mặc dù VPN là một giải pháp truy nhập từ xa rất tốt nhưng bạn cũng có thể sử dụng nó để tách biệt các khu vực cần có độ bảo mật cao với phần còn lại của mạng doanh nghiệp. Ví dụ, không có lý do gì tất cả nhân viên của công ty lại cần truy nhập đến các máy chủ và máy trạm trên mạng của phòng Nhân sự. Tất nhiên là một số người thì cần nhưng đại đa số thì không. Trong trường hợp đó, bạn có thể đặt một máy chủ Microsoft VPN ở "lề" mạng của phòng Nhân sự và yêu cầu tất cả các nhân viên của công ty phải kết nối tới mạng đó qua L2TP/IPSec. L2TP/IPSec yêu cầu các máy phải được xác thực bằng chứng chỉ số và bạn có thể tăng cường bảo mật bằng cách yêu cầu xác thực cả người sử dụng.

5. Chính sách hạn chế phần mềm

Chính sách hạn chế phần mềm (software restrictions policy) của Microsoft cho phép bạn kiểm soát những chương trình chạy trên máy tính của bạn. Bạn có thể tạo một chính sách ngăn không cho một số loại phần mềm nào đó chạy trong thư mục tải tệp đính kèm trong chương trình thư điện tử của bạn nếu bạn lo ngại người nhận thư sẽ nhận được những thư có đính kèm virus. Trong một máy tính có nhiều người sử dụng, bạn cũng có thể chỉ cho phép một số người nào đó được quyền truy nhập tới một số loại tệp nhất định.

Chính sách hạn chế phần mềm cũng cho phép bạn kiểm soát những ai có thể add trusted publisher vào những máy tính được quản lý. Sử dụng chính sách hạn chế phần mềm, bạn có thể ngăn không cho phép bất kỳ tệp nào chạy trên máy tính của bạn, tổ chức của bạn hoặc miền của bạn. Ví dụ, nếu có một loại virus đã biết, bạn có thể sử dụng chính sách hạn chế phần mềm để ngăn cản máy tính của bạn mở những tệp có chứa virus.

6. Ngăn cách miền IPSec

Ngăn cách miền IPSec là một phương pháp kiểm soát các giao vận giữa tất cả các máy tính trên mạng Active Directory của bạn. Các hệ thống máy trạm có thực sự cần thiết kết nối tới tất cả các máy chủ trên mạng của bạn? Liệu có phải tất cả các máy chủ, thậm chí những máy chủ ở trong cùng một vùng bảo mật cần phải kết nối tới nhau? Tất nhiên là không. Mặc dầu phần lớn chúng ta thiên về việc nghĩ IPSec là một phương pháp bảo mật, nó sẽ chiếm ít công suất xử lý của máy tính hơn trong khi vẫn đạt hiệu quả tương đương nếu bạn không triển khai việc mã hoá.

7. Máy chủ Xác thực Internet

Máy chủ xác thực Internet (Internet Authentication Server) là phiên bản Radius của Microsoft, cho phép bạn xác thực tất cả những người sử dụng agaist Active Directory của bạn từ những máy không phải là thành viên của miền. Nó đặc biệt hữu dụng đối với các truy nhập mạng LAN, các kết bối VPN truy nhập từ xa và xác thực máy khách Web proxy. IAS là một phần của hệ điều hành Windows 2003 và bạn có thể cài đặt hoặc gỡ bỏ nó một cách dễ dàng.

8. Lọc TCP/IP

Các phiên bản Windows 2000 và Windows 2003 đều có tính năng lọc TCP/IP cho phép bạn kiểm kiểm soát các kết nối theo giao thức và số cổng. Bạn có thể thấy tính năng này trong hộp thoại Advanced TCP/IP Properties (thẻ Options). Bạn có thể cấu hình tính năng lọc TCP/IP để cho phép người sử dụng chỉ truy nhập đến một số cổng (TCP, UDP) hay một số giao thức nào đó (bằng cách xác định mã số của giao thức). Tính năng lọc TCP/IP có thể áp dụng cho tât cả các cổng (interface) trên máy tính. Một trong những hạn chế của tính năng này là nó không cho phép chặn hoặc kiểm soát các thông điệp ICMP.