**Không rõ**

Bảo mật Windows Registry: Ngăn chặn khả năng tấn công từ xa

Chào mừng các bạn đón đọc đầu sách từ dự án sách cho thiết bị di động  
  
*Nguồn:* [*http://vnthuquan.net/*](http://vnthuquan.net/)  
Tạo ebook: Nguyễn Kim Vỹ.

**MỤC LỤC**

[Bảo mật Windows Registry: Ngăn chặn khả năng tấn công từ xa](" \l "bm2)

**Không rõ**

Bảo mật Windows Registry: Ngăn chặn khả năng tấn công từ xa

Mặc dù được coi là "trái tim" của hệ điều hành, nhưng theo mặc định Registry trong tất cả các hệ thống Windows vẫn được "mở cửa" tự do và có thể tiếp cận thông qua mạng Internet hoặc mạng nội bộ. Một hacker kỹ thuật có khả năng sử dụng điểm yếu này để tấn công vào hệ thống máy tính của bạn, hoặc cơ quan bạn. Chính vì vậy, để đảm bảo an toàn, bạn cần phải vô hiệu hoá con đường tiếp cận này.  
Chú ý: Do có thể phát sinh rủi ro nên trước khi chỉnh sửa Registry, bạn cần phải tiến hành backup thành phần này.    
Sửa đổi Registry   
Đối với Windows 2000, Windows XP, và Windows Server 2003:  
   
Start --> Run.   
Gõ Regedt32.exe, và click OK.   
Tìm tới:  
HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet  
\Control\SecurePipeServers.   
Nếu khoá winreg đã có sẵn, bạn sẽ chuyển tới thực hiện bước 8; còn nếu không có, bạn cần tạo mới giá trị này bằng cách chọn Edit --> Add Key.   
Đặt tên khoá mới là winreg, lớp REG\_SZ.   
Chọn khoá mới, rồi chọn Edit --> Add Value.   
Nhập các thông số sau:   
Name: Description  
Type: REG\_SZ  
Value: Registry Server   
    
Chọn khoá winreg, và chọn Security --> Permissions.   
Bạn có thể thêm, bớt hoặc bỏ quyền của các tài khoản được liệt kê.    
Đóng cửa sổ Registry Editor, và khởi động lại máy tính.    
Chú ý:   
+ Nếu bạn có một nhóm tài khoản hoạt động trên máy chủ và máy trạm mà không thuộc nhóm quản trị, bạn cần cấp quyền thích hợp cho các tài khoản này.   
+ Nếu hệ thống bạn đang tiến hành thay đổi là máy chủ hoặc hệ thống cho phép thực hiện kết nối từ xa đối với người dùng hợp pháp, bạn phải cấp quyền truy cập cho các tài khoản dịch vụ liên quan tới khoá winreg.    
Sửa đổi mạng  
Ngoài cách can thiệp trực tiếp và Registry, bạn cần thực hiện một số công việc khác liên quan tới đường mạng để bảo đảm an toàn cho hệ thống. Đó là khoá các cổng: TCP/UDP 135, 137, 138, 139, và 445 ngay tại router hoặc ứng dụng tường lửa. Phong toả các cổng này sẽ không chỉ vô hiệu hoá khả năng truy cập từ xa tới registry mà còn ngăn không cho tin tặc thực hiện các cuộc tấn công hệ thống Windows từ xa.   
Tắt các cổng trên cũng sẽ giúp bạn tăng tốc khả năng hoạt động của hệ thống. Tuy nhiên, trước khi thực hiện bạn cần phải chắc rằng sẽ không còn cần các dịch vụ liên quan tới các cổng trên

Lời cuối: Cám ơn bạn đã theo dõi hết cuốn truyện.  
Nguồn: http://vnthuquan.net  
Phát hành: Nguyễn Kim Vỹ.  
  
Nguồn: Theo VDC  
Được bạn: mickey đưa lên  
vào ngày: 5 tháng 12 năm 2004