10 thiết lập Group Policy quan trọng trên Windows cần thực hiện ngay

Một trong những phương pháp phổ biến để cấu hình máy Microsoft Windows là sử dụng Group Policy. Đây là những thiết lập liên quan tới đăng ký trên máy tính, cấu hình các thiết lập bảo mật và hành vi khi vận hành máy. Group Policy có thể mở từ Active Directory (từ client) hoặc cấu hình ngay trên máy (local). Máy Windows 8.1 và Windows Server 2012 R2 có tới hơn 3.700 thiết lập cho hệ điều hành.

Dưới đây là **10 thiết lập Group Policy quan trọng** mà bạn cần quan tâm. Không phải chỉ nên dừng lại ở 10 thiết lập này vì mỗi thiết lập hợp lý đều giúp giảm rủi ro. Nhưng 10 lựa chọn này sẽ quyết định hầu như tất cả.

Nếu thiết lập đúng cho 10 cái tên này, bạn sẽ tạo ra một môi trường Windows an toàn hơn. Tất cả đều nằm trong mục **Computer Configuration/Windows Setting/Security Settings.**

1. Đổi tên tài khoản Local Administrator

Nếu kẻ xấu không biết tên tài khoản admin, họ sẽ mất nhiều thời gian hơn để hack. Đổi tên tài khoản admin không thể làm tự động mà bạn phải tự làm.

2. Vô hiệu hóa tài khoản khách

Một trong những điều tệ nhất bạn làm chính là bật tài khoản này. Nó trao nhiều quyền truy cập vào máy Windows và không cần mật khẩu. Rất may là có lựa chọn vô hiệu hóa tính năng này mặc định,

Thiết lập Group Policy đúng để bảo đảm an toàn cho máy Windows

3. Vô hiệu hóa LM và NTLM v1

LM **(LAN Manager)** và giao thức chứng thực NTLM v1 rất dễ bị tấn công. Hãy sử dụng **NTLM v2** và **Kerberos.** Mặc định, hầu hết mọi máy Windows đều chấp nhận cả 4 giao thức. Trừ phi bạn có máy cổ (hơn 10 năm) và chưa được vá thì hiếm khi lại nên dùng giao thức cũ. Có thể mặc định vô hiệu hóa chúng.

4. Vô hiệu hóa lưu trữ LM

Hash mật khẩu LM rất dễ bị chuyển sang dạng plain text. Đừng để Windows lưu chúng trên ổ đĩa, nơi hacker có thể dùng công cụ để tìm ra. Nó được vô hiệu hóa mặc định.

5. Độ dài mật khẩu tối thiểu

Độ dài mật khẩu cho người dùng bình thường nên là ít nhất 12 kí tự - 15 kí tự hoặc hơn với những tài khoản cấp cao hơn. Mật khẩu Windows là không an toàn lắm nếu có dưới 12 kí tự. Để an toàn nhất trong thế giới chứng thực của Windows thì nên là 15. Như vậy gần như sẽ đóng mọi cửa sau.

Rất tiếc là thiết lập Group Policy cũ chỉ có tối đa 14 kí tự. Hãy dùng **Fine-Grained Password Policies,** tuy không dễ thiết lập và cấu hình trên Windows Server 2008 R2 (và đời cũ hơn) nhưng với WIndows Server 2012 về sau thì rất dễ.

6. Tuổi thọ tối đa của mật khẩu

Mật khẩu từ 14 kí tự trở xuống không nền dùng lâu hơn 90 ngày. Thời hạn mật khẩu tối đa mặc định của Windows là 42 ngày, nên bạn có thể dùng số này hoặc tăng lên 90 ngày nếu muốn. Một số chuyên gia an ninh cho rằng dùng mật khẩu tới 1 năm cũng không sao nếu nó có 15 kí tự trở lên. Dù vậy hãy nhớ là thời hạn càng lâu thì rủi ro ai đó đánh cắp và dùng nó để truy cập tài khoản khác của cùng một người là càng cao. Dùng trong thời hạn ngắn vẫn tốt hơn.

7. Event Logs

Nhiều nạn nhân bị tấn công đã có thể phát hiện sớm nếu bật Event Logs và có thói quen kiểm tra chúng. Hãy đảm bảo bạn sử dụng thiết lập được khuyến nghị trong công cụ **Microsoft Security Compliance Manager** và sử dụng **Audit Subcategories.**

8. Vô hiệu hóa điểm danh SID nặc danh

Security Identifiers (SID - mã nhận diện bảo mật) là những con số được chỉ định cho mỗi người dùng, nhóm và đối tượng bảo mật trên Windows hoặc **Active Directory.** Ở những bản Windows đầu tiên, người dùng chưa được chứng thực có thể truy vấn những con số này để xác định người dùng quan trọng (như quản trị viên) và nhóm, các hacker rất thích khai thác điều này. Điểm danh này có thể được vô hiệu hóa mặc định.

9. Đừng để tài khoản nặc danh nằm trong nhóm mọi người

Thiết lập này cùng thiết lập trước đó khi bị cấu hình sai sẽ cho phép kẻ nặc danh truy cập hệ thống xa hơn cho phép. Cả hai thiết lập đều có thể bật mặc định (vô hiệu hóa truy cập nặc danh) từ năm 2000.

10. Bật kiểm soát tài khoản người dùng (User Account Control - UAC)

Kể từ Windows Vista, UAC là công cụ bảo vệ số 1 khi duyệt web. Tuy vậy nhiều người lại tắt đi do thông tin cũ về vấn đề tương thích phần mềm. Hầu hết các vấn

đề này đã không còn, những gì còn lại có thể giải quyết bằng tiện ích phát hiện không tương thích miễn phí của Microsoft. Nếu vô hiệu hóa UAC, bạn sẽ gặp nguy hiểm nhiều hơn trên Windows NT so với các OS mới hơn. UAC được bật mặc định.

Các bản OS mới được thiết lập mặc định đúng khá nhiều

Nếu để ý bạn sẽ thấy 7 trên 10 thiết lập này đã được cấu hình đúng trên Windows Vista, Windows Server 2008 và các bản về sau. Không cần lãng phí thời gian tìm hiểu cả 3.700 thiết lập Group Policy, hãy cấu hình đúng 10 thiết lập trên là được.