GIỚI THIỆU VỀ ĐIỀU KHIỂN TOÀN VẸN TRONG WINDOWS VISTA

Khi cá

Khi các chuyên gia phát triển phần mềm tại Microsoft bắt tay vào xây dựng phiên bản mới nhất của hệ điều hành, Windows Vista, họ đã bắt tay vào để xây dựng sao cho nó là một phiên bản bảo mật tốt nhất từ trước đến nay của Windows. Một trong những chức năng được cài đặt sẵn bên trong Windows Vista làm cho nó trở nên an toàn hơn đó là điều khiển toàn vẹn WIC (Windows Integrity Control).

Mục đích của WIC là để bảo vệ các đối tượng, cho dù chúng là các file, máy in, pipe được đặt tên, registry key khỏi các kẻ tấn công, malware hoặc thậm chí là các lỗi của người dùng. Khái niệm WIC được dựa trên việc thiết lập tính đáng tin cậy của các đối tượng khác nhau và việc điều khiển tương tác giữa các đối tượng dựa vào tính toàn vẹn của chúng.

Các mức toàn vẹn của WIC là một điều khiển có tính bắt buộc và các điều khiển được sử dụng để ghi đè như sự cho phép của file và folder NTFS mà các quản trị viên đã rất thân thuộc. Đối tượng chính của WIC là bảo đảm rằng chỉ các đối tượng có mức toàn vẹn bằng hoặc hơn với đối tượng mục tiêu mới được phép tương tác với nó. Về bản chất, nếu một đối tượng nào đó kém tin tưởng thì nó sẽ bị ngăn chặn hành động hoặc việc tương tác với các đối tượng tin cậy hơn.

WIC đóng vai trò chính cho những cho phép bình thường. Điều đó nghĩa là cho dù một file hoặc quá trình nào đó có sự cho phép điều khiển hoàn chỉnh với đối tượng khác, nhưng nếu file này hoặc quá trình này có mức toàn vẹn thấp hơn đối tượng mà nó đang cố gắng tương tác với thì WIC sẽ ghi đè sự cho phép và tương tác sẽ bị từ chối.

Việc xác định tính tin cậy bằng sử dụng WIC

Để kiểm soát được các tương tác giữa các đối tượng, Windows trước tiên phải xác định được sự tin cậy hoặc mức toàn vẹn của mỗi đối tượng. WIC sẽ gán một trong sáu mức toàn vẹn sau cho mỗi một đối tượng:

• Không tin cậy – Các quá trình được đăng nhập nặc danh sẽ tự động bị chỉ định như một quá trình không tin cậy.

• Thấp – Mức toàn vẹn thấp là mức được sử dụng mặc định cho tương tác với Internet. Khi Internet Explorer sử dụng trong trạng thái mặc định, chế độ được bảo vệ, tất cả các file và quá trình kết

hợp với nó được gán cho mức toàn vẹn thấp. Nhiều folder như Temporary Internet Folder cũng mặc định bị gán cho mức toàn vẹn thấp.

• Trung bình – Mức trung bình là mức mà hầu hết các đối tượng sẽ được sử dụng. Những người dùng chuẩn nhận được mức toàn vẹn trung bình này và bất kỳ đối tượng nào không rõ ràng trong việc chỉ định cho mức toàn vẹn cao hơn hay thấp hơn đều được gán mặc định mức trung bình này.

• Cao – Các quản trị viên được cho phép có mức toàn vẹn cao. Điều này bảo đảm rằng các quản trị viên có khả năng tương tác và có thể thay đổi đối tượng đã gán mức toàn vẹn thấp hoặc trung bình nhưng cũng có thể thực hiện hành động trên các đối tượng khác với một mức toàn vẹn cao, những hành động này không có đối với người dùng chuẩn.

• Hệ thống – Như tên hàm ý của nó, mức toàn vẹn hệ thống được dành riêng cho hệ thống. Nhân Windows và các dịch vụ bên trong lõi được cho phép ở mức này. Mức này là mức cao hơn mức cao của các quản trị viên để bảo vệ các chức năng khỏi bị ảnh hưởng hoặc bị tổn thương.

• Bộ cài – Mức bộ cài là một trường hợp đặc biệt và là mức toàn vẹn cao nhất. Hiệu lực của nó bằng hoặc cao hơn tất cả các mức toàn vẹn WIC khác, các đối tượng đã được gán cho mức này có thể Uninstall tất cả đối tượng khác.

Bằng việc thiết lập mặc định mức toàn vẹn trung bình cho người dùng chuẩn và cho tất cả các đối tượng không được gán nhãn, Vista bảo vệ phần lớn đối tượng trên máy tính tránh bất kỳ ảnh hưởng nào của các mối đe dọa từ Internet.

Cũng giống như vậy, các quản trị viên có nhiều quyền ưu tiên hơn người dùng chuẩn và được hoạt động tại mức toàn vẹn cao, nhân hệ điều hành và các chức năng lõi với mức toàn vẹn cao hơn, việc bảo đảm rằng một quản trị viên vô tình hoặc tài khoản của quản trị viên có thể không ảnh hưởng bất lợi đến hệ thống lõi.

Để lặp lại, các mức toàn vẹn WIC và điều khiển cũng giống như sự cho phép folder và file NTFS. Sự khác nhau chính ở đây là những cho phép NTFS là các điều khiển được sử dụng trong khi mức toàn vẹn WIC là điều khiển có tích chất bắt buộc. Về cơ bản, các đặc quyền và sự cho phép truy cập file và folder được gán bởi đối tượng sở hữu hoặc một quản trị viên trong khi mức toàn vẹn WIC được chỉ định bởi hệ điều hành.

Khi bốn mức trên được sử dụng ít trong thực tế, thì sự khác nhau giữa mức thấp và mức trung bình là ở chỗ chức năng của WIC. Việc bổ sung các điều khiển có tính chất bắt buộc được sử dụng nhiều hơn là dựa vào người dùng hoặc quản trị viên hiển nhiên đã cho thấy vấn đề bảo mật tốt hơn tại tất cả các mức. Nhưng khả năng để cô lập các file và quá trình từ Internet và bảo vệ máy tính chống lại malware trong Internet là một trong những lý do chính cho sự tồn tại của WIC.

Bảo vệ Vista khỏi các mối đe dọa trong Internet

Trong khi người dùng chuẩn được hoạt động ở mức toàn vẹn trung bình và quản trị viên được hoạt động trong mức cao thì WIC thừa nhận rằng Internet và các file hoặc quá trình liên quan đến nó hoàn toàn không đáng tin và mặc định gán chúng ở mức toàn vẹn thấp.

Khi người dùng nhận được emai có liên kết đến một website nguy hiểm (loại email mà chúng ta cần phải xóa) và người này lại nhấn chuột vào nó, website hiểm độc này có thể cài đặt một hay nhiều loại malware nguy hiểm vào máy tính của người này. Malware sẽ copy chính bản thân nó đến nhiều vị trí khác trên ổ cứng và thay đổi Registry key để bảo đảm nó được tồn tại liên tục. Mặt khác nó cũng có thể thay đổi hoặc xóa file hoặc thực thi quá trình để tiến hành các hành động nguy hiểm.

Trong Windows XP hoặc các hệ thống cũ, rất khó khăn để có thể bảo vệ hệ thống đối với malware. Còn với Windows Vista, mọi thứ liên quan đến Internet được hoạt động tại mức toàn vẹn thấp, malware sẽ không thể thay đổi, xóa hoặc tương tác với bất kỳ thứ gì trong hệ thống.

Sử dụng chế độ bảo vệ

Tự động đặt mức toàn vẹn thấp trên Internet Explorer đang hoạt động trong chế độ bảo vệ. Chế độ bảo vệ đã được nói đến như một trong những nâng cấp bảo mật đáng kể trong Windows Vista và trong Internet Explorer 7. Khi chế độ bảo vệ được bật thì mọi chức năng trong Internet Explorer sẽ mặc định được gán với mức toàn vẹn thấp.

Nhiều trang web có thể không chạy đúng chức năng hạn chế được đặt trong chế độ bảo vệ. Bạn hoàn toàn có thể vào tab Security trong Internet Options để bỏ chọn tùy chọn 'Enable Protected Mode'. Việc làm này sẽ xóa bỏ hầu hết các tính năng bảo vệ của Vista đã cung cấp để chống lại các hành động trái phép và nguy hiểm thông qua Internet. Tuy nhiên chúng tôi khuyên bạn nên để chế độ bảo mật trong trạng thái "On".

Khi hoạt động kinh doanh, khả năng cho phép hoặc vô hiệu hóa chế độ bảo vệ là vấn đề cần làm, vấn đề này được gỡ bỏ bởi sử dụng Group Policy. Đối với người dùng đơn lẻ thì việc vô hiệu hóa chế độ bảo vệ để truy cập vào các trang mà có các vấn đề được sử dụng nhiều, đơn giản chỉ bằng cách thêm các trang này vào vùng bảo mật tin cậy trong Internet Explorer. Mỗi một vùng bảo mật trong Internet Explorer đều có cấu hình bảo mật duy nhất và vùng tin cậy hoạt động với chế độ bảo vệ đã bị vô hiệu hóa một cách mặc định.

Sử dụng ICACLS để quan sát các mức toàn vẹn

Một trong những vấn đề mà các quản trị viên gặp phải khi giải quyết các vấn đề sao cho đúng và sự cho phép trong môi trường Windows để tìm ra các vấn đề mà ai đó đang truy cập. Nếu một quá trình nào đó bị thất bại thì một file sẽ không được thực thi hoặc người dùng không thể ghi dữ liệu vào folder, một trong những phương pháp xử lý sự cố có thể là kiểm tra mức toàn vẹn WIC của đối tượng trong câu hỏi và đối tượng đang cố gắng hành động để xác định có WIC nào ẩn sau hay không.

Windows Vista không cung cấp chức năng để bạn có thể quan sát hoặc thay đổi mức toàn vẹn của một đối tượng. Tuy vậy, tiện ích dòng lệnh ICACLS sẽ hiển thị các nội dung của CAL cũng như các nhãn bắt buộc. Các đối tượng không được gán rõ ràng một nhãn sẽ tự động được chỉ định mức toàn vẹn trung bình, mặc dù vậy nhãn toàn vẹn trung bình sẽ không hiển thị việc sử dụng ICACLS bởi vì nó được hàm ý và không dứt khoát.

Để sử dụng tiện ích ICACLS, trước tiên bạn phải mở một cửa sổ lệnh. Có một số các chuyển tiếp và cú pháp để sử dụng công cụ ICACLS. Bạn có thể có được thông tin và chi tiết trên mỗi tùy chọn sử dụng chúng đơn giản bằng việc đánh 'icacls' tại cửa sổ lệnh và nhấn phím Enter. Chúng ta sẽ tập trung vào hai ứng dụng ICACLS ở đây.

Đầu tiên, quan sát mức toàn vẹn. Để quan sát mức toàn vẹn và các nội dung khác của danh sách truy cập tùy ý, bạn đánh icacls sau đường dẫn của đối tượng muốn kiểm tra. Ví dụ: nếu bạn muốn quan sát mức toàn vẹn có tính cách bắt buộc của file explorer.exe thì bạn đánh icacls c:\windows\explorer.exe. Kết quả sẽ nhận được như nội dung trong hình dưới.

```
C:\windows\explorer.exe    NT SERVICE\TrustedInstaller:(F)
                           BUILTIN\Administrators:(RX)
                           NT AUTHORITY\SYSTEM:(RX)
                           BUILTIN\Users:(RX)
```

Như trên, mức toàn vẹn có tính chất bắt buộc đã gán cho file explorer.exe được hàm ý rằng nó không được gán mức toàn vẹn bắt buộc cụ thể. Nếu có mức toàn vẹn bắt buộc cụ thể thì sẽ có thêm một mục nhập như dưới đây:

Mandatory Label\Medium Mandatory Level

Bạn cần phải biết rằng nếu bạn đang sử dụng ICACLS để thử và xác định mức toàn vẹn bắt buộc được sử dụng để xác định đối tượng tương tác trong WIC, còn nếu không có nhãn bắt buộc nghĩa là nó được gán cho mức trung bình mặc định.

Hoàn toàn có thể thay đổi một mức toàn vẹn của đối tượng bằng việc sử dụng ICACLS. Để làm điều này, một người dùng phải được gán SeRelabelPrivilege. Để thay đổi mức toàn vẹn của một đối tượng, người dùng cần phải có thẩm quyền để thay đổi cũng như có được quyền sở hữu của đối tượng mục tiêu. Miễn là các đặc quyền này thỏa đáng thì người này có thể thay đổi hoặc nâng mức toàn vẹn của một đối tượng. Mặc dù vậy, người dùng không thể thiết lập đối tượng đến mức tòan vẹn cao hơn ngoài thẩm quyền.

Với việc thừa nhận có sự cho phép đúng đắn và đặc quyền, bạn có thể thay đổi mức toàn vẹn của một đối tượng với công cụ ICACLS bằng việc đánh icacls /setintegritylevel H|M|L. Nhãn ở cuối H, M hoặc L tương ứng được gán mức toàn vẹn cao, trung bình và thấp.

An toàn hơn với WIC

Khi nói đến việc bảo mật dữ liệu trên máy tính Windows, một trong những biến số không thể dự đoán và không thể điều khiển được đó là thành phần con người. Ngày nay, các tổ chức đã bắt đầu nhận ra rằng, người dùng không thể phụ thuộc vào việc phân loại hợp thức và mã hóa thông tin nhạy cảm vì vậy có một xu hướng đang phát triển mã hóa đĩa trên các thiết bị tính toán di động đặc biệt và gỡ bỏ các biến.

WIC cũng hoạt động tương tự. Người dùng có khả năng quản lý các file/folder và gán đặc quyền cho phép nhóm hoặc cá nhân riêng lẻ có thể xem, điều chỉnh, xóa hoặc thực hiện các hành động của họ. Mặc dù vậy, các điều khiển truy cập tùy ý vẫn phải đưa ra các thông báo hỏi để đảm bảo chắc chắn người dùng đang thực hiện hoạt động đó.

Có nhiều sự cải thiện có thể được tạo ra, ví dụ: việc cung cấp sự quản lý và công cụ cấu hình tốt hơn công cụ dòng lệnh ICACLS. Bảo mật được cung cấp bởi WIC là không hoàn hỏa nhưng nó tốt hơn chế độ bảo mật của các phiên bản Windows trước đó và nó bảo vệ hệ thống Vista tránh được nhiều mối đe dọa có thể ảnh hưởng đến Windows XP, Windows 2000 hoặc các hệ điều hành trước đó.