LỖ HỔNG GMAIL - "GÓT CHÂN ASIN" CỦA WEB 2.0

Khi mộ

Khi một lỗ hổng trong thiết kế phần mềm xây dựng trên nền Web Google hồi đầu tuần này bị phát hiện, tất thảy mọi người đều giật mình trước xu hướng đáng lo ngại về bảo mật đối với các lĩnh vực IT.

Đó là cần phải làm gì để bảo vệ hệ thống nội bộ cũng như các dữ liệu quan trọng, khi nhân viên sử dụng dịch vụ email hoặc những phần mềm hợp tác phải dùng tới máy tính của chủ doanh nghiệp.

Trục trặc về bảo mật của Google Mail được công bố lần đầu trên trang web Googlified. Theo đó, những rắc rối bắt đầu nảy sinh từ cách thức phần mềm Google lưu trữ thông tin trong một file JavaScript trên server của công ty này.

Trước khi Google tiến hành cài đặt miếng vá thì một tin tặc hoàn toàn có thể viết đè lên JavaScript Object Notation, hay còn gọi là JSON, yếu tố Google sử dụng để gửi thông tin từ server của nó tới máy của người dùng và dành quyền truy cập tới tất cả những thông tin liên lạc lưu trong tài khoản Gmail của người dùng, miễn là người dùng đó đã đăng nhập vào Google. Hiện tượng này gọi là "giả mạo các yêu cầu giữa các site" (Cross-site request forgery).

Nhờ có JSON mà các trình web mail có khả năng tự động điền địa chỉ trong trường "To:" ở phần soạn thư như vẫn thấy, tức là khi người dùng chỉ cần đánh một vài chữ trong phần địa chỉ người nhận đã lưu trong danh sách, ngay lập tức JSON sẽ giúp hoàn thiện đầy đủ mà không phải đánh hết.

Hãng Google cũng thừa nhận, vào những ngày cuối tuần đầu năm mới này, họ đã nhận được cảnh báo về sự cố liên quan tới việc sử dụng các đối tượng JSON gây ảnh hưởng tới rất nhiều sản phẩm của công ty. Ông Heather Adkins, nhà quản lý bảo mật thông tin của Google cho biết: "Những đối tượng đó nếu bị lạm dụng sẽ làm phơi bày thông tin một cách không chủ ý". Google thông báo đã sửa chữa sự cố đó trong vòng 24 giờ kể từ khi nhận được thông báo.

Ông Gary McGraw, trưởng phòng công nghệ của Cigital, nhà cung cấp dịch vụ an ninh Web bình luận: "Google đã sửa sai rất nhanh, và điều đó cũng khiến bạn hiểu rằng vấn đề là hết sức nghiêm trọng". Cũng theo ông này thì lỗ hổng bảo mật mới bị phát hiện của Google chính là "mở đầu cho hàng loạt những vấn đề sẽ xảy ra khi người ta quá coi trọng SOA cũng như web 2.0,

những công nghệ dựa trên ngôn ngữ JavaScript, client-side mở rộng và tính năng dựa vào trình duyệt".

Tất nhiên đa số các chuyên gia bảo mật đều đồng ý với quan điểm, bảo vệ các phần mềm ứng dụng web là tối quan trọng vì một nền thịnh vượng chung của cả hệ thống lẫn an toàn dữ liệu, nhưng họ vẫn tranh cãi với nhau ở điểm, liệu các lỗ hổng bảo mật trong những trình ứng dụng web phục vụ khách hàng như web mail, tán gẫu và mạng xã hội ảo kiểu như MySpace và Facebook có phải là mối hoạ tiềm ẩn với hệ thống IT của doanh nghiệp hay không.

Các nhân viên thì cứ "hồn nhiên" sử dụng web mail và các dịch vụ web khác trên máy tính làm việc của họ, trong khi đó những người đảm trách nhiệm vụ quản lý IT thì lại hầu như không thể nắm được độ bảo mật của những trình ứng dụng web đó. Chuyên gia phân tích cao cấp của tập đoàn Yankee, ông Andrew Jaquith cho rằng, chính những gì không ta không hiểu về trình ứng dụng web đã khiến chúng tiềm ẩn rất nhiều nguy cơ.

Ông nói: "Vì chúng không được hiểu đầy đủ nên chúng sẽ thu hút được mối quan tâm rất lớn của các tin tặc". Ông cũng cho rằng, "thực tiễn này cũng sẽ khiến các nhà quản lý IT phải bận tâm nhiều vì các trình ứng dụng phục vụ khách hàng đang ngày càng trở thành những bộ phận thiết thực trong cơ sở hạ tầng IT tập thể".

Điều này cũng có nghĩa các nhân viên có lúc còn "tống" cả đống thông tin liên quan tới công việc vào kho lưu trữ dữ liệu khổng lồ do các hệ thống web mail quản lý. Một ví dụ rất đơn giản là thế này, khi một nhân viên nào đó không thể nhớ được password của trang web nào đó, họ liền đánh password đó ra rồi gửi tới tài khoản web mail để có thể truy cập vào website từ bất kỳ máy tính có nối mạng nào.

Mọi việc sẽ chẳng có gì để nói nếu như không xảy ra trường những password kiểu này có thể truy cập được vào các trang liên quan tới công việc, và khi đó, bảo mật cho web mail sẽ trở thành vấn đề hết sức "đau đầu".

"Các tài khoản web mail sẽ cho phép bạn truy cập vào mọi thứ", đó là nhận xét của ông Jeremiah Grossman, sáng lập viên đồng thời là CTO của WhiteHat Security, hãng sáng chế phần mềm đánh giá bảo mật trình ứng dụng web. Ông Grossman cũng đã từng làm việc cho Yahoo với tư cách là nhân viên bảo mật.

Theo ông này, các giả mạo yêu cầu liên trang không chỉ được sử dụng để câu trộm thông tin từ các tài khoản web mail, bởi hơn thế nữa, các tin tặc sẽ truy cập được vào bất cứ tài khoản nào mà người dùng đã truy cập qua, kể cả các tài khoản ngân hàng".

Một tình huống đáng nghi ngại khác cũng được đặt ra là trường hợp tin tặc lấy trộm ID và password của người dùng web mail rồi giả mạo gửi thư tới các đồng nghiệp của họ. Ông McGraw giải thích thêm: "Tất cả những tin tặc đều phải làm một việc là gửi email tới những đồng nghiệp của người dùng, trong đó có thể viết, "hôm nay tôi làm việc ở nhà cho nên hãy trao đổi công việc với tôi qua email". Thủ đoạn này có thể sẽ thu được một mẻ lưới lớn khi rất nhiều thông

tin liên quan đến công việc sẽ chuyển về tài khoản email đó.

Tuy nhiên, các chuyên gia bảo mật khác vẫn coi việc nhân viên sử dụng web mail làm rò rỉ tin tức quan trọng của doanh nghiệp một cách vô tình hay cố ý vẫn nguy hiểm hơn chuyện doanh nghiệp đó bị malware tấn công.

Chuyên gia phân tích cao cấp Nick Selby của tập đoàn 451 lý giải: "Những trình ứng dụng nào mà nhân viên của bạn sử dụng không dưới quyền kiểm soát của bộ phận IT trong công ty đều trở thành những bận tâm đáng kể về vấn đề bảo mật. Còn khi doanh nghiệp của bạn bị tin tặc dùng malware cài bẫy, bạn có thể xác định được điều đó khi kiểm tra các điểm cuối, nếu quả thực có chuyện đó thì chỉ cần cô lập các điểm cuối bị nhiễm malware mà thôi".

Hiện tại thì cả Google, Yahoo và nhiều hãng cung cấp dịch vụ web khác đều đang rất say sưa với những tính năng "trên cả tuyệt vời" của Web 2.0 được xây dựng trên nền JavaScript, họ cũng sẽ rất nhanh chóng khắc phục các lỗ hổng bảo mật dù rằng chẳng thể "hân hoan" mỗi khi phải đón nhận những thông tin như Googlified chỉ ra đây. Thôi thì có thể chuyện các nhà quản lý IT ngừng sử dụng các trình ứng dụng web sẽ là điều không tưởng nhưng họ vẫn cần hết sức cảnh giác trước những nguy cơ thất thoát dữ liệu và thiệt hại hệ thống đang chờ thời "tạo tác".

Đỗ Dương