5 phương thức bảo mật cho các dự án nguồn mở

Dễ nhận thấy, các phần mềm nguồn mở dường như là "món hời" cho các doanh nghiệp nhỏ và vừa. Tất cả đều miễn phí và có sẵn trên Internet - điều đặc biệt đáng giá với ngân sách hạn hẹp của những doanh nghiệp này. Và quan trọng hơn cả, phần mềm nguồn mở được cho là có tính bảo mật cao hơn so với các phần mềm thương mại bán sẵn.

Thế nhưng, theo thời gian, liệu phần mềm nguồn mở có duy trì được khả năng bảo mật vốn có?

Câu trả lời là có, bởi mã nguồn là mở và được sử dụng, bổ sung, sửa chữa không ngừng bởi rất nhiều các nhà phát triển và chuyên gia phần mềm trên toàn cầu. Tuy nhiên, cũng giống như các sản phẩm thương mại ở bên kia "chiến tuyến", phần mềm nguồn mở vẫn cần được gia cố, cập nhật các bản vá lỗi cả trước và sau khi đã triển khai.

Dưới đây là những kinh nghiệm thực tiễn quan trọng mà các doanh nghiệp nhỏ và vừa nên tuân theo để đảm bảo các ứng dụng nguồn mở của mình luôn trong trạng thái an toàn và bảo mật.

LẬP SỔ QUẢN LÝ PHẦN MỀM

Nếu doanh nghiệp của bạn chưa có sổ quản lý phần mềm, hãy thiết lập ngay. Sổ phần mềm cung cấp phương thức quản lý và kiểm soát các phần mềm đang được sử dụng trong doanh nghiệp của bạn. Ngay cả với những công ty nhỏ, số lượng phần mềm ứng dụng, kể cả nguồn mở và thương mại, vẫn có thể vượt quá khả năng kiểm soát nếu không được ghi chép đầy đủ. Trong khi mua các phần mềm thương mại bạn sẽ được cung cấp hoá đơn để sử dụng cho mục đích lưu giữ và tra cứu sau này, thì các phần mềm nguồn mở lại dễ dàng được tải về từ Internet mà không để lại bất cứ "dấu vết"nào.

Bạn không những nên ghi lại ngày giờ tải về phần mềm mà còn cần kiểm tra tính toàn vẹn của các phần mềm nguồn mở được tải về trước khi tiến hành cài đặt. Các phần mềm nguồn mở thường đi kèm với mã băm MD5 hoặc chữ kí GNU Privacy Guard nhằm giúp người dùng kiểm tra việc tải về có hoàn tất và đầy đủ không. Nếu phần mềm gặp lỗi khi kiểm tra tính toàn vẹn và phải tải lại, điều này cũng cần được ghi chép lại trong sổ quản lý phần mềm.

QUẢN LÝ VIỆC VÁ LỖI

Quản lý vá lỗi cho các phần mềm nguồn mở khá phức tạp nhưng là công việc không thể bỏ qua. Thời gian phát hành các bản vá lỗi thường không đồng bộ với lịch cập nhật của bạn khiến cho việc lập kế hoạch vá lỗi trở nên khó khăn. Tuy nhiên không phải không có cách để dàn xếp ổn thoả.

Đối với các doanh nghiệp nhỏ và vừa sử dụng không quá nhiều phần mềm nguồn mở, thực hiện vá lỗi thủ công là giải pháp kinh tế nhất, nếu không muốn nói đó là lựa chọn duy nhất. Bạn cần thực hiện kiểm tra và tiến hành vá lỗi một cách thủ công cho các ứng dụng như Apache hay Jakarta do đây là

các sản phẩm thường xuyên phát hành bản vá lỗi nhưng lại thiếu khả năng cập nhật tự động như của hệ thống Linux.

Một lựa chọn khác cho các doanh nghiệp nhỏ và vừa là sử dụng một đoạn mã lệnh (script) định kỳ kiểm tra Website của phần mềm nguồn mở và tự động cài đặt bản vá lỗi. Hầu hết các quản trị viên hệ thống đều có khả năng viết đoạn mã lệnh như vậy và thiết lập để nó tự động thực thi theo những khoảng thời gian nhất định, vào lúc máy tính rỗi – chẳng hạn cuối tuần hoặc lúc nửa đêm.

Tuy nhiên, khi doanh nghiệp phát triển tới quy mô lớn hơn, việc cập nhật vá lỗi thủ công hay thông qua mã lệnh không còn khả thi. Lúc đó, các công cụ quản lý vá lỗi là bước đi tiếp theo. Thế nhưng không may là hầu hết các phần mềm quản lý vá lỗi đều chỉ có khả năng cập nhật cho Windows. Chỉ một số ít các sản phẩm cập nhật được cho phần mềm nguồn mở như PatchLink Update hay NetChk Protect của Shavlik Technologies.

KIỂM TRA KHẢ NĂNG TƯƠNG THÍCH MẠNG VÀ TƯỜNG LỬA

Cũng giống như các phần mềm khác, phần mềm nguồn mở có thể yêu cầu mở một số cổng TCP nhất định để truy cập mạng Internet. Hãy kiểm tra lại để chắc chắn rằng khi thực hiện như vậy sẽ không tạo ra lỗ hổng bảo mật nào trong mạng của bạn.

Bên cạnh đó, một điểm quan trọng là phần mềm nguồn mở cần tương thích với kiến trúc bảo mật mạng hiện có của doanh nghiệp. Nếu việc sử dụng một ứng dụng nguồn mở nào đó đòi hỏi những thay đổi đáng kể về kiến trúc làm ảnh hưởng tới khả năng bảo mật của mạng, có lẽ bạn cần cân nhắc lại liệu nó có phù hợp với tổ chức của mình không và tìm kiếm các giải pháp thay thế khác.

QUẢN LÝ TRUY CẬP

Bạn cần thay đổi tất cả các thiết lập bảo mật mặc định ngay khi cài đặt xong phần mềm nguồn mở nhằm tránh cặp mắt dòm ngó của các tin tặc – những

người luôn có sẵn trong tay danh sách các tên đăng nhập và mật khẩu thông dụng.

Ngoài ra, nếu có thể hãy nâng cấp hệ thống quản lý truy cập có sẵn trong phần mềm nguồn mở. Chẳng hạn phần mềm máy chủ Apache sử dụng phương thức xác thực cơ bản và mã hoá (digest authentication) có thể bị các tin tặc xuyên thủng, cùng tập tin "htaccess" để cung cấp khả năng bảo vệ bằng mật khẩu khi truy xuất một thư mục trên Website. Đừng chỉ dựa vào các phương thức này bởi có nhiều cách tốt hơn để hạn chế truy cập, chẳng hạn sử dụng các tập tin cấu hình hay các mô-đun bảo mật của Apache, hoặc khoá truy cập trên máy chủ thông qua hệ điều hành.

KIỂM TRA VÀ RÀ SOÁT LỖ HỔNG

Các bộ công cụ của Fortify Software và Ounce Labs có thể quét các lỗ hổng phần mềm, trong khi WebInspect của SPI Dynamics và AppScan của Watchfire có thể kiểm tra các lỗ hổng trong Website sử dụng Apache hay các phần mềm máy chủ Web nguồn mở khác.

Xét một cách toàn diện, phần mềm nguồn mở có tính bảo mật cao hơn so với các giải pháp thương mại, tuy nhiên người dùng cần có sự quan tâm cần thiết nhằm đảm bảo các quy trình cài đặt, cấu hình và vá lỗi được thực thi một cách an toàn. Các doanh nghiệp nhỏ và vừa với tài chính và nguồn lực hạn chế cần luôn đổi mới – sáng tạo vượt trên các doanh nghiệp lớn, và phần mềm nguồn mở chính là giải pháp thích hợp trong hoàn cảnh này.

Quang Dũng