5 LỖI THƯỜNG GẶP TRONG QUẢN LÝ LỖ HỔNG BẢO MẬT

Trong con mắt của một số người vấn đề quản lý các lỗ hổng được xem là một trong những hoạt động quản lý bảo mật chuyên sâu. Lại có một số người khác cho rằng đây chỉ là một quá trình cần thiết mà Microsoft phải làm để cho ra các bản vá cập n

Trong con mắt của một số người vấn đề quản lý các lỗ hổng được xem là một trong những hoạt động quản lý bảo mật chuyên sâu. Lại có một số người khác cho rằng đây chỉ là một quá trình cần thiết mà Microsoft phải làm để cho ra các bản vá cập nhật hàng tháng. Và cũng có không ít người xem đây chỉ là một "cụm từ marketing thông dụng" của các nhà kinh doanh. Thông qua bài viết sau đây chúng tôi muốn điểm lại một số lỗi thông thường mà các tổ chức nên chú ý để nhằm đạt được sự hoàn thiện trong quản lý lỗ hổng bảo mật trên cả phương diện công nghệ và quy trình. 1. Quét nhưng không có bất kì hành động gì Lỗi thông thường đầu tiên chính là việc quét và do tìm các lỗi bảo mật nhưng lại không có bất kì một hành động phản ứng nào với các kết quả thu được từ quá trình trên. Các chuyên gia quét và dò tìm lỗi bảo mật đã trở thành những "chiếc kẹp" trong rất nhiều các tổ chức. Công nghệ quét và dò tìm lỗ hổng bảo mật thực sự đã phát triển mạnh và trưởng thành trong những năm gần đây với minh chứng là tính chính xác, tốc độ và mức độ an toàn của những công cụ đã được cải thiện đáng kể. Tuy nhiên, các công cụ quét thương mại hiện đại hay mã nguồn mở hiện nay vẫn mắc một căn bệnh tương tự như các hệ thống phát hiện cảnh báo sớm (IDS). Thứ nhất, những công cụ kiểu này quá ồn ào vì nhiều lý do khác nhau mà chúng sản sinh ra quá nhiều các cảnh báo. Thêm vào đó, chúng lại không hề nói cho bạn biết là bạn phải làm gì để xử lý các cảnh báo lỗ hổng bảo mật kia cũng như các IDS không nói cho bạn biết bạn phải quan tâm đến một cảnh báo đột nhập cụ thể nào. Do vậy mà quản lý lỗ hổng bảo mật không phải là việc quét và dò tìm mà điều quan trọng ở đây phải là những việc làm sau khi thực hiện công việc quét và dò tìm. Công việc này bao gồm kiểm kê tài nguyên, ưu tiên và nghiên cứu các hoạt động khắc phục cũng như các hành động thực tế như vá hay cấu hình lại hoặc bảo vệ. 2. Xem việc vá lỗ hổng bảo mật là công việc tương tự như quản lý lỗ hổng bảo mật Thực tế, công việc vá các lỗ hổng bảo mật là cách thức sửa chữa các lỗ hổng bảo mật đã được đã được biết đến. Thậm trí một số các chuyên gia trong ngành còn cho rằng việc quản lý các lỗ hổng bảo mật là rất đơn giản chỉ bao gồm việc cho vá-sửa mọi vấn đề rắc rối là xong. Nhưng có rất nhiều các lỗ hổng bảo mật không thể sửa hay vá chỉ bằng cách đơn giản cập nhật phiên bản mới nhất các ứng dụng mà còn đòi hỏi việc phải thay đổi hay cấu hình lại nhiều thông số hệ thống. Do vậy mà công việc quản lý lỗ hổng bảo mật được sinh một yêu cầu cần phải ưu tiên và sửa chữa một cách thông minh các lỗ hổng bảo mật được phát hiện bằng phương pháp vá hay bất kì một phương pháp nào khác. Vì thế nếu bạn bận vào mọi phút giây trong ngày thứ 3 nhưng không làm bất kì việc gì để loại bỏ mọi lỗ hổng bảo mật trong doanh nghiệp trong suốt 29 ngày còn lại của tháng thì bạn thực sự chưa làm công việc quản lý lỗ hổng bảo mật. 3. Cho rằng quản lý lỗ hổng bảo mật chỉ là một vấn đề kĩ thuật Nếu bạn nghĩ rằng quản lý lỗ hổng bảo mật chỉ đơn giản là một vấn đề kĩ thuật thì đó thực sự là một điều rất đáng ngạc nhiên. Nhằm đạt được hiệu quả trong công việc này nó cần có sự liên hệ chú ý tới việc cải thiện chính sách và quy trình. Trên thực tế việc tập trung vào quy trình và mặt "mềm" trong các câu đố lỗ hổng bảo mật thường mang lại nhiều lợi ích hơn là một hệ thống vá lỗ công nghệ cao. Có thể nói hiện vẫn tồn tại khá nhiều điểm yếu trong các chính sách cũng như hạ tầng công nghệ thông tin. Ở đây chúng tôi cũng xin không đề cập đến những yếu kém trong chính sách – đây đôi khi cũng được coi là lỗ hổng bảo mật. Lấy ví dụ, nếu bạn không kiên quyết thực hiện một chính sách yêu cầu mật khẩu có độ dài theo quy định thì đó chính

là yếu kém hay lỗ hổng trong chính sách của bạn và những chuyên gia quét và dò tìm có thể sẽ không phát hiện ra và hậu quả là sẽ không có bất kì giải pháp nào cho vấn đề này. Do vậy, mật khẩu yếu, thiếu nhận thức về tính bảo mật dữ liệu cũng như việc thiếu các chuẩn cấu hình máy trạm sẽ có thể mang lại nhiều thiệt hại hơn cho bức tranh bảo mật của bạn cũng như gia tăng các nguy cơ mà bạn phải đối mặt. Theo các chuyên gia phân tích Gartner thì: "Quy trình quản lý lỗ hổng bảo mật phải bao gồm các công việc như định nghĩa chính sách, xác định danh giới môi trường, ưu tiên, bảo vệ, giảm nhẹ thiệt hai cũng như việc giám sát và bảo trì." Như vậy, theo cách hiểu trên thì quy trình quản lý lỗ hổng bảo mật sẽ bắt đầu bằng một văn bản định nghĩa chính sách về các vấn đề như tài nguyên của tổ chức - ứng dụng hay hệ thống – cùng với người sử dụng. Một văn bản như thế này cùng với các quy trình bảo mật khác phải xác định được quy mô của quản lý lỗ hổng bảo mật cũng như xác định các giai đoạn "được xem là tốt" của các nguồn tài nguyên công nghệ thông tin. 4. Đánh giá một lỗ hổng bảo mật mà không nhìn vào bức tranh toàn cảnh Những người cố gắng tuân thủ một quy trình quản lý lỗ hổng bảo mật hợp lý đôi khi lại mắc phải lỗi thông thường này. Như khi họ phải đối mặt với thách thức nghiêm trọng trong việc ưu tiên sửa các lỗ hổng bảo mật họ lại thường bỏ qua các góc độ nguy hiểm của sự ưu tiên đó. Lấy ví dụ như họ cố gắng tiếp cận tìm hiểu sự quan trong của các lỗ hổng bảo mật chỉ dựa trên chính các lỗ hổng bảo mật đó thôi mà không nhìn vào bức tranh toàn cảnh mối đe doạ bảo mật đó cũng như các vai trò kinh doanh của hệ thống bị ảnh hưởng. Chỉ có một cách duy nhất để tránh mắc phải lỗi thông thường thứ tư này chính là sử dụng công thức Risk = Threat x Vulnerability x Value (Nguy cơ = Đe doạ x Lỗ hổng bảo mật x Giá trị) và sử dụng các kết quả của công thức tính này để quyết định xem phải ưu tiên vá lỗ hổng nào trước. Nhưng để có thể xác lập thứ tự ưu tiên vá các lỗ hổng bảo mật một cách thông minh bạn cần phải quan tâm đến những yếu tố khác trong trong môi trường công nghệ thông tin của chính bạn cũng như môi trường bên ngoài thế giới. Những yếu tố này bao gồm: - Sự nguy hiểm của các lỗ hổng bảo mật - Các thông tin có liên quan đến mối đe doạ bảo mật - Giá trị kinh doanh và thông tin về các hệ thống mục tiêu Gần đây, một chuẩn mới trong việc phân loại mức độ nguy hiểm của các lỗ hổng bảo mật đã được đưa ra giới thiệu giúp cho các tổ chức trong việc ưu tiên thứ tự các lỗ hổng cần phải sửa. Common Vulnerability Scoring System (CVSS - Hệ thống tính điểm lỗ hổng bảo mật thông thường) xem xét đa dạng các đặc điểm của lỗ hổng bảo mật như tính ưu tiên, khả năng bị khai thác và ảnh hưởng. CVSS được hứa hẹn là sẽ cung cấp một phương thức thống nhất trong việc tính điểm đánh giá các lỗ hổng bảo mật và sẽ sớm được nhiều nhà cung cấp thông tin bảo mật áp dụng. Tuy nhiên, dữ liệu CVSS vẫn cần phải được nâng cấp bổ sung thêm thông tin về giá trị kinh doanh cũng như các mối đe doạ. Thông tin kinh doanh là sự sống còn trong việc tính toán thứ tự ưu tiên các lỗ hổng bảo mật vì chúng có khả năng kết hợp các mối đe doạ kĩ thuật và lỗ hổng dữ liệu thành một chức năng kinh doanh. Các tổ chức khác nhau về mọi khía cạnh đặc điểm và như vậy họ có những tài sản quản trọng và ứng dụng khác nhau. Các cuộc tấn công ảnh hưởng đến một số các tổ chức có thể làm họ bị phá sản nhưng với một số tổ chức khác thì đó chỉ có thể là sự giám đoạn tạm thời. Tuy nhiên, trên thực tế cuộc sống không hề đơn giản như thế và các lỗ hổng bảo mật các lỗ hổng bảo mật không có tính quan trọng cao đôi khi là là viêc đá lót đường cho việc tận dung khai thác một lỗ hổng bảo mật khác quan trọng hơn. 5. Không được chuẩn bị kĩ càng cho điều chưa biết đến - Lỗi bảo mật zero-day Lỗi thông thường thứ năm chính là lỗi bảo mật "zero-day exploit". Lỗi bảo mật này chính là nỗi sợ hãi của rất nhiều các nhà quản lý bảo mật. Trong khi tôi vẫn còn thấy rất nhiều sự bối rối băn khoăn về việc cái gì làm nên "zero-day exploit"? Đơn giản chỉ là việc khai thác một lỗ hổng bảo mật chưa từng được công bố trước đây. Vì thế cho dù bạn đã vá mọi lỗ

hổng bảo mật được biết đến thì bạn vẫn cần phải chuẩn bị cho các cuộc tấn công bởi những kẻ tấn công sử dụng các lỗ hổng bảo mật chưa từng đươc biết đến. Bạn cần phải làm gì? Bên cạnh một chương trình quản lý lỗ hổng bảo mật nhạy cảm bao gồm một khối lượng các công việc có thể bảo vệ bạn khỏi các "zero-day exploit" và giảm sát cẩn thận sự bảo mật mạng máy chủ. Bên cạnh đó bạn cũng cần bảo đảm là mọi kế hoạch đáp trả phải luôn sẵn sàng trong trường hợp bị tấn công. Những tình huống như thế này cần phải được giải quyết bằng cách sử dụng nguyên tác "bảo mật theo chiều sâu" trong các thiết kế cơ sở hạ tầng bảo mật.