SQL INJECTION LẬP KỶ LỤC TẤN CÔNG CSDL

Số lượng các vụ tấn công nhằm vào cơ sở dữ liệu (CSDL) web đã lên tới một con số kỷ lục trong năm nay khi mà tin tặc thấy đây chính là "một hũ mật ngọt" các thông tin tài chính và cá nhân của người dùng. Hãng bảo mật Se

Số lượng các vụ tấn công nhằm vào cơ sở dữ liệu (CSDL) web đã lên tới một con số kỷ lục trong năm nay khi mà tin tặc thấy đây chính là "một hũ mật ngọt" các thông tin tài chính và cá nhân của người dùng. Hãng bảo mật SecureWorks cho biết đã phát hiện tới 8.000 vụ tấn công lên các cơ sở dữ liệu mỗi ngày. Như vậy, con số này đã tăng thêm trung bình từ 100 đến 200 vụ tấn công một ngày so với con số của 3 tháng đầu năm. Con số thống kê của SecureWorks được thống kê từ hệ thống các cơ sở dữ liệu của hơn 1.300 khách hàng sử dụng các giải pháp dịch vụ bảo mật của hãng này. SecureWorks cho biết tin tặc - chủ yếu sử dụng các máy tính tại Nga, Trung Quốc, Brazill, Hungary và Hàn Quốc - hiện đều dùng chung một phương pháp có tên SQL Injection trong những vụ tấn công vào các cơ sở dữ liệu. Jon Ramsey - kỹ sư công nghệ trưởng của SecureWorks - cho biết tin tặc trước hết sẽ sử dụng Google để tìm kiếm các trang web có chứa form nhập liệu còn hoạt động. Đây chính là đầu mối giúp chúng có thể gửi các thông tin vào cơ sở dữ liệu mục tiêu. Trong khi đó, rất nhiều các ứng dụng web thường không kiểm tra thông tin đầu vào từ các form nhập liệu. Chính điều này đã giúp cho tin tặc có thể chèn các mã lệnh SQL độc hại vào cơ sở dữ liệu. Từ đó tin tặc có thể sử dụng các công cụ để thu thập thông tin từ một số bảng và cột nhất định trong cơ sở dữ liệu. Bước kế tiếp trong việc tấn công cơ sở dữ liệu là tin tặc sẽ chèn thêm các mã lệnh điều khiển máy chủ cơ sở dữ liệu tải về các phần mềm khác trên Internet giúp chúng có được quyền kiểm soát cao hơn đối với mục tiêu. SQL Injection là kiểu tấn công có mục tiêu rất cụ thể và thường là mục tiêu đơn lẻ cho mỗi một vụ tấn công. Chính vì thế mà những vụ tấn công như thế này thường không gây được sự chú ý rộng rãi như virus hay sâu máy tính. Thiệt hại khôn lường Âm thầm như thế nhưng thiệt hại của những vụ tấn công này lại rất lớn. Nếu như một máy chủ cơ sở dữ liệu bị tin tặc chiếm quyền kiểm soát thì sẽ có một khối lượng rất lớn thông tin cá nhân tài chính của người dùng sẽ rơi vào tay chúng. Và nếu thành công thì có thể nói nguồn thông tin mà tin tặc thu được còn nhiều hơn rất nhiều so với tấn công phishing. Tin tặc không phải mất công giả mạo để lừa người sử dụng cung cấp thông tin cá nhân tài chính. Tỉ lệ thành công của các vụ tấn công SQL Injection thường rất cao. "Hiện chúng ta không phải ở trong thời đại của sâu máy tính, mà chúng ta đang ở trong thời đại của các lỗi zero-day và những vụ tấn công nhắm mục tiêu rất cụ thể," Ramsey khẳng định. Doanh nghiệp cần phải nghiêm túc xem xét lại tính bảo mật hệ thống cơ sở dữ liệu của mình trước khi trở thành nạn nhân của các vụ tấn công SQL Injection. Visa International và MasterCard International hiện cũng đang phải soạn thảo lại các nguyên tắc bảo mật trong việc chấp nhận thanh toán bằng thẻ tín dụng nhằm chống lại các vụ tấn công SQL Injection. Một trong những vụ tấn công SQL Injection nổi tiếng nhất chính là vụ tấn công vào CardSystems Solutions - một hãng chuyên lưu trữ có sở dữ liệu thanh toán thẻ tín dụng. Tin tặc đã sử dụng giải pháp tấn công SQL Injection để chiếm quyền điều khiển hệ thống cơ sở dữ liệu của CardSystems và chuyển toàn bộ cơ sở dữ liệu ra ngoài. Đã có khoảng 40 triệu thẻ tín dụng rơi vào tay chúng gây ra thiệt hại hàng triệu USD. Hoàng Dũng