KHÁCH HÀNG MOBIFONE CÓ THỂ BỊ LỘ THÔNG TIN CÁ NHÂN?

Vừa qua, một cảnh báo của VSEC cho hay: "Website của MobiFone đang có lỗ hổng nghiêm trọng, dẫn đến tình trạng thông tin bí mật của khách hàng bị rò rỉ" (!?). Để biết rõ thực hư nhằm bảo vệ quyền lợi của người tiêu dùng, chúng tôi đã c&ugr

Vừa qua, một cảnh báo của VSEC cho hay: "Website của MobiFone đang có lỗ hổng nghiêm trọng, dẫn đến tình trạng thông tin bí mật của khách hàng bị rò rỉ" (!?). Để biết rõ thực hư nhằm bảo vệ quyền lợi của người tiêu dùng, chúng tôi đã cùng chuyên gia bảo mật Phùng Anh Tuấn của VSEC đến trực tiếp trụ sở của MobiFone để trao đổi vấn đề này. Thông tin khách hàng bị rò rỉ?

Chuyên gia bảo mật mạng Phùng Anh Tuấn đang chỉ ramột lỗi bảo mật của mạng MobiFone tại trụ sở MobiFone

Hệ thống website MobiFone cho phép khách hàng của mạng này có thể đăng ký tài khoản sử dụng thông qua website để quản lý tài khoản cước điện thoại của mình. Ngoài ra, khách hàng có thể sử dụng account trực tuyến để nhắn tin, tải logo, hình ảnh, nhạc chuông và tiền sẽ được tính vào cước sử dụng của khách hàng. Hệ thống admin (quản trị) của MobiFone được truy cập thông qua http://www.mobifone.com.vn/admin. Hệ thống cấm tất cả các IP bên ngoài đăng nhập vào, cho dù người đó có thông tin password (mật khẩu) đúng mà chỉ cho phép 1 máy bên trong hệ thống mạng LAN có địa chỉ IP cố định truy cập vào hệ thống. Tuy nhiên, theo cảnh báo của VSEC, khi phân tích được lỗi của hệ thống website, hacker có thể truy cập vào hệ thống admin một cách dễ dàng. Trong hệ thống admin của website, sau khi kiểm soát được hệ thống cơ sở dữ liệu, hacker có thể sử dụng tài khoản của khách hàng khác ở trên server để nhắn tin, trong khi tiền bị trừ vào tài khoản của người đó. Nghiêm trọng hơn, theo cảnh báo, hacker có thể tự động tạo account của bất cứ số điện thoại nào thuộc mạng MobiFone để kiểm soát thông tin của số điện thoại đó thông qua hệ thống website dù người chủ của số điện thoại chưa bao giờ truy cập vào website MobiFone. Ngoài ra, hacker cũng có thể kiểm soát những thông tin quan trọng của tất cả các khách hàng như số điện thoại gọi đi, thời gian đàm thoại, v.v… "Hacker không thể làm được điều đó!" Trả lời phóng viên, ông Nguyễn Tuấn Huy - Phó phòng Tin học tính cước MobiFone lại cho rằng trang admin này chỉ có thể truy nhập bằng máy nội bộ. Bởi người sử dụng phải cầm điện thoại có sim bên trong, gửi tin nhắn dựa trên tin nhắn nhập mã xác thực mới có thể đăng ký dịch vụ, từ đó mới có thể lấy được thông tin cá nhân, cước và số điện thoại gọi đến được" - Ông Huy khẳng định - "Nếu không có máy và sim thì hacker không thể kích hoạt được account. Không có bất kỳ tool (phương tiện) nào để tạo accout cả". Theo đó, hacker không thể tạo được tài khoản của khách hàng khác ở trên server để thực hiện nhắn tin hoặc sử dụng các chức năng có trên hệ thống website. Theo các nhân viên kỹ thuật của MobiFone, đã có nhiều trường hợp vợ cầm máy của chồng rồi lấy password để đăng ký dịch vụ xem cước chi tiết hoặc để nhắn tin. Điều này hoàn toàn có thể xảy ra nếu thuê bao để máy ở nhà. "Thời điểm đầu khi mới triển khai dịch vụ này, chúng tôi nhận được nhiều thông tin khách hàng phàn nàn tại sao tài khoản lại bị trừ tiền trên website. Về sau mới phát hiện ra rằng họ đã vô tình bị người khác "mượn" điện thoại" - một nhân viên kỹ thuật phòng Tin học tính cước nói. Tuy nhiên, trước sự chứng kiến và đồng ý của các nhân viên phòng Tin học tính cước MobiFone, chuyên gia Phùng Anh Tuấn đã trình diễn kỹ thuật cho thấy web server có lỗ hổng. Theo giải thích của Phùng Anh Tuấn, đây là lỗi của Oracle 9iAS JEE Webserver (9.0.3.0.0) cho phép hacker có thể tải bất cứ file JSP nào trên hệ thống website về, giúp hacker nghiên cứu và nắm được hệ thống website www.mobifone.com.vn. Ngoài ra, lỗi này còn cho phép hacker thực hiện lệnh truy vấn thông tin máy chủ để xem cấu trúc thư mục, file trên

server. Trong khi đó, các chuyên gia tin học của MobiFone vẫn yêu cầu Phùng Anh Tuấn tiếp tục trình diễn lấy thông tin của một số điện thoại bất kỳ tại chỗ. Nhưng yêu cầu trên đã bị từ chối. Lý giải về sự từ chối này, Phùng Anh Tuấn cho biết: "Đây là vấn đề thuộc về pháp lý, chúng tôi chỉ là những người làm bảo mật mạng, phát hiện nguy cơ và gửi cảnh báo tới vì quyền lợi của hàng triệu thuê bao. MobiFone nên tự rà soát lại toàn bộ hệ thống website của họ. Nếu Mobifone không tin và muốn chúng tôi chứng minh, họ cần phải có công văn yêu cầu gửi tới VSEC". Trao đổi với phóng viên, ông Nguyễn Tuấn Huy cho hay, ngay sau khi nhận được sự cảnh báo của VSEC, MobiFone đã huy động các chuyên gia tin học, an ninh mạng rà soát và triển khai các biện pháp kỹ thuật đảm bảo an toàn cho website. Ông Huy tiết lộ, trước đây họ đã từng phát hiện một hacker quấy rối và đã áp dụng các biện pháp răn đe cần thiết. Ông Huy nhấn mạnh: "Nhà chúng tôi có khóa, mọi hành động xâm nhập dù thiện chí hay không đều là bất hợp pháp".