HỆ THỐNG TÊN MIỀN DNS SERVER CỦA BẠN BỊ CẤU HÌNH SAI?

Nghiên cứu chỉ ra rằng hơn một nửa số lượng DNS server bị cấu hình sai. Các nguy cơ bảo mật theo đó cũng tăng lên. Hơn một nửa dịch vụ tên miền Internet bị cấu hình sai, để lại nhiều lỗ hổng mạng cho các cuộc tấn công pharming, khiến các server bị lợi dụng trong các cuộc tấn c
Nghiên cứu chỉ ra rằng hơn một nửa số lượng DNS server bị cấu hình sai. Các nguy cơ bảo mật theo đó cũng tăng lên. Hơn một nửa dịch vụ tên miền Internet bị cấu hình sai, để lại nhiều lỗ hổng mạng cho các cuộc tấn công pharming, khiến các server bị lợi dụng trong các cuộc tấn công có thể phá huỷ hoàn toàn cơ sở hạ tầng của hệ thống tên miền (DNS). Đó là nội dung chính của cuộc khảo sát các dịch vụ tên miền Internet mới được công bố hôm thứ hai. Cuộc khảo sát này do Measurement Factory tiến hành để chuẩn bị cho Infoblox, hãng sẽ bán các thiết bị liên quan đến DNS tới đây. Tình hình bảo mật tên miền tệ đến mức báo cáo DNS Report Card 2006 chỉ cho được đến điểm D+ (trong thang điểm theo thứ tự chữ cái A, B, C, D…, A là cao nhất). Đây là cuộc khảo sát thường niên thứ hai do Measurement Factory tiến hành nhằm tìm hiểu tình hình hệ thống tên miền mở rộng. "Chúng tôi nhìn thấy các cuộc tấn công tăng cường phát triển từng bước về cả số lượng và tính chất khốc liệt, cũng như kết quả chẳng mấy hay ho từ các cấu hình tệ hại trong cơ sở hạ tầng DNS", Rick Kagan - phó giám đốc makerting ở Infoblox nói. Cái được nhất từ cuộc khảo sát là tìm ra hơn một nửa dịch vụ tên miền Internet cho phép đệ quy tên dịch vụ. Kiểu giải pháp tên này thường đòi hỏi một name server để tiếp nhận yêu cầu tới các server name khác. Infoblox nói rằng việc cho phép các dịch vụ tên đệ quy để lại nhiều lỗ hổng mạng ẩn giấu các cuộc tấn công độc hại. Người dùng thường sẽ bị chuyển hướng sang một website khác thay vì website muốn sử dụng và thường hay bị mất thông tin cá nhân. "Các server không cần hỗ trợ dịch vụ tên đệ quy", Kagan nói. "Vấn đề là BIND 9 lại cho phép đặt chế độ dịch vụ tên đệ quy mặc định… Một lỗ hổng tồi tệ. Nó đã bị khai thác và có nhiều minh chứng phổ biến về tình hình này. Sửa chữa không khó, mọi người nên lưu lại dạng lỗ hổng này". Một vấn đề của cấu hình DNS khác cũng được tìm ra trong cuộc khảo sát là có tới 29% dịch vụ DNS cho phép truyền vận theo vùng (zone transfer) tới các máy có yêu cầu bất kỳ. Các truyền vận zone transfer sẽ copy dữ liệu DNS từ một dịch vụ tới dịch vụ khác, để mở cơ hội khai thác cho các cuộc tấn công DoS (denial-of-service). Một số kết quả khác từ cuộc khảo sát:

Số lượng dịch vụ DNS kết nối Internet tăng 20% , lên tới con số 9 triệu trong năm 2005. Hầu hết đều tăng ở châu Âu và châu Á với nhiều dịch vụ DNS mới được nhúng trong modem cáp và cổng vào điện thoại.

Số lượng dịch vụ DNS sử dụng phần mềm nguồn mở mới nhất (BIND 9 của Internet Software Consortium được sử dụng nhiều hơn so với phiên bản cũ của nó là BIND 8) tăng từ 58% trong năm 2005 lên đến 61% tính đến thời điểm này của năm nay.

Cứ trong 1.000 dịch vụ DNS chỉ có 2 dịch vụ hỗ trợ IP Version 6, thể hiện một bước tiến chậm, dần dần nâng cấp thành các giao thức truyền thông chính của Internet.

Các công nghệ ảo hoá đang sử dụng DNSSEC, tiêu chuẩn được đề nghị dùng để thẩm định dữ liệu DNS. DNSSEC được hỗ trợ trong số 100.000 dịch vụ DNS.

T.Thu