BẢO VỆ SERVER DNS TRƯỚC HACKER NHƯ THẾ NÀO

Mạng c

Mạng của chúng ta thường được bảo vệ bởi một phần mềm tường lửa. Nhưng người tiền nhiệm của tôi đã đặt cả máy chủ quản lý hệ thống tên miền chính/phụ (DNS server primary/secondary), chịu trách nhiệm xử lý các miền ra ngoài thế giới mạng được bảo vệ bởi tường lửa. Có cách nào tốt nhất trong việc bảo vệ DNS server trước các vị khách không mời mà đến? (Lượm lặt từ Internet).

Đã có một số, tuy không nhiều cách được đưa ra trong vấn đề ngăn chặn nguy hiểm cho DNS server trước hacker. Bạn nên đặt DNS server sau một tường lửa hiện thời và cung cấp cho chúng địa chỉ IP. Khi cho phép cổng 53 được đi qua tường lửa, chắc chắn rằng cả TCP và UDP cũng phải được qua. Tôi rút ra bài học "xương máu" này khi lần đầu tiên đặt các server DNS sau một tường lửa. Nhiều vấn đề ngắt quãng trong giải pháp hệ thống tên miền (DNS) liên tục xuất hiện cho đến khi TCP và UDP được đi qua tường lửa ở cổng 53.

Nếu server DNS đã ở sau tường lửa hiện thời, bạn nên đặt chúng trong một subnet khác với mạng con của tập hợp server hay thiết bị nào đó đã có trên mạng. Bạn cũng nên đặt lệnh lập danh sách điều khiển truy cập trên switch của mạng con DNS server cư ngụ. Điều này không cho phép lưu lượng được chuyển tới cổng vào trên mạng mà chỉ thực hiện qua kết nối Internet. Lựa chọn khác là đặt server trên kết nối DMZ. Một số tường lửa cho phép sử dụng tuỳ chọn này, nhưng phải cài đặt thêm card mạng bổ sung nếu tường lửa không có cổng phụ sử dụng được.

Hoặc, bạn có thể đặt DNS server sau một tường lửa riêng không kết nối với mạng. Như thế, nếu tường lửa hoặc không DNS server nào bị xâm phạm, mạng của bạn không gặp phải nguy hiểm gì, vì kết nối này không trực tiếp. Nếu cài đặt thêm DNS server thứ ba (giả sử tới thời điểm đó mới chỉ có 2 DNS server), bạn có thể thực hiện tuỳ chọn bảo vệ khác. Trong cấu hình này, cả hai DNS server đều là hệ thống DNS phụ. Thông tin DNS trên server không thể thay đổi trực tiếp. Các thay đổi không qua thẩm định chỉ kéo dài đến khi server phụ nhận được bản update từ server chính mới đã cài đặt. Để thực hiện thành công, server DNS chính không cung cấp địa chỉ IP chung và được cấu hình chỉ liên lạc với DNS server phụ.

Phần mềm DNS bạn đang sử dụng có thể cho phép một số tuỳ chọn thêm khác. Ví dụ, Bind 9 hỗ trợ thành phần gọi chương trình xem, ngăn chặn DNS server đưa ra ngoài giải pháp hệ thống tên miền trên các domain server không được cấu hình để cung cấp thông tin trực tiếp. Có nghĩa là, đây không phải là nguồn server DNS chung ai cũng có thể sử dụng. Lưu lượng mở rộng có thể

được “can ngăn” sử dụng DNS server cho các miền chúng không phục vụ.