GIẢI PHÁP MỚI TĂNG CƯỜNG BẢO MẬT CHO DỊCH VỤ VOIP QUA CÁP

Ngày 12/4/2006, Tập đoàn Juniper Networks đã công bố một giải pháp mới giúp các nhà khai thác đa hệ thống dịch vụ qua cáp (MSOs) bảo vệ các dịch vụ dựa trên giao thức SIP và VoIP trước những cuộc tấn công mạng. Giải pháp mới tăng cường khả năng bảo

Ngày 12/4/2006, Tập đoàn Juniper Networks đã công bố một giải pháp mới giúp các nhà khai thác đa hệ thống dịch vụ qua cáp (MSOs) bảo vệ các dịch vụ dựa trên giao thức SIP và VoIP trước những cuộc tấn công mạng. Giải pháp mới tăng cường khả năng bảo mật của những dịch vụ hiện tại, đồng thời giúp giảm thiểu các chi phí do lỗi mạng và cung cấp các dịch vụ. Làm việc với bất cứ hệ thống cổng modem dùng cáp theo chuẩn PacketCable Multimedia (CMTS) nào, giải pháp Hạn chế Đe doạ Động qua Cáp gồm tổ hợp các thiết bị định tuyến, các thiết bị Phát hiện và Phòng chống xâm nhập (IDP) và Hệ thống Triển khai Dịch vụ SDX, cho phép các MSOs nhận dạng và cô lập một cách nhanh chóng, hiệu quả các mối đe doạ bảo mật, đồng thời gửi cảnh báo máy đã bị nhiễm đến các khách hàng và những nhân viên điều hành. Với việc sử dụng kiến trúc dựa trên CMTS, giải pháp Hạn chế Đe dọa Động qua Cáp mới của Juniper giúp các MSOs bảo mật các dịch vụ VoIP trên toàn hệ thống mạng của họ, từ lõi IP cho đến người sử dụng cuối. Giải pháp Hạn chế Đe doạ Động qua Cáp sử dụng một thiết bị IDP của Juniper Networks, thiết bị này giám sát những cuộc tấn công mạng ở mỗi người sử dụng, mỗi ứng dụng, hoặc dựa trên những nhu cầu, đồng thời sử dụng sản phẩm SDX 300 của Juniper Network. Lưu lượng xấu như phần mềm nguy hại (malware) hay tấn công từ chối dịch vụ phân tán (DDoS) sẽ được IDP phát hiện và phát tín hiệu cảnh báo tới SDX-300. SDX sau đó sẽ phát ra một chính sách thích hợp đến bất cứ thiết bị định tuyến nào của Juniper Networks và/hoặc hệ thống cổng modem dùng cáp theo chuẩn PacketCable Multimedia hay thiết bị định tuyến của bên thứ ba, giúp các MSOs triển khai một loạt những lựa chọn để giảm thiểu các mối đe dọa.

Tùy theo bản chất của những đe dọa, các MSOs có thể lựa chọn để giới hạn hay lọc lưu lượng, làm rớt cuộc gọi hoặc kết nối lại với người sử dụng tới cổng web và tự động khởi tạo lại dịch vụ khi các đe doạ được loại trừ. Bên cạnh việc bảo mật các dịch vụ VoIP, giải pháp mới cũng có thể được mở rộng để cung cấp tính bảo mật cho các dịch vụ dựa trên giao thức SIP, như trò chơi điện tử trực tuyến (game online), hội nghị truyền hình, dịch vụ tin nhắn nhanh (IM) và những dịch vụ bấm-gọi (push-to-talk). SIP thường là mục tiêu của tấn công từ chối dịch vụ (DoS), tấn công giả mạo và nhiều cuộc tấn công khác.