GIAÌ PHAP PHONG VỆ THEO LỚP CHO MẠNG VOIP

Do VoI

Do VoIP hoạt động trên cơ sở hạ tầng IP nên dễ bị tấn công. Lý thuyết ma`hãng Juniper đưa ra bắt đầu bằng các phương pháp hiệu quả nhất trong bảo mật mạng và tương tự như đối với bất cứ mạng IP nào khác.

Việc đầu tiên là phải nắm rõ tất cả những thành phần liên quan bao gồm các máy chủ, giao thức IP, quy trình, người sử dụng và dùng một mẫu phân tích rủi ro để xác định những nguy cơ nằm ở đâu. Sau đó chọn ra công nghệ hay quy trình phù hợp để giảm thiểu các rủi ro.

Trung tâm mạng của doanh nghiệp hay nhà cung cấp dịch vụ đều đặt trong máy chủ ứng dụng VoIP hay server UNIX hoặc PC chạy hệ điều hành Linux. Mạng lõi cũng có các máy chủ đang vận hành chương trình quản lý dữ liệu người dùng và cước phí nhằm hỗ trợ ứng dụng VoIP.

Tại vùng biên là các gateway servers, những máy chủ liên lạc với các server mạng VoIP khác hoặc chuyển những cuộc gọi giữa các mạng thoại chuyển mạch và VoIP. Còn máy khách chính là điện thoại IP chuyển tín hiệu số thành âm thanh.

Nguồn: checkpoint

Chiến lược phòng vệ của Juniper nằm trong các lớp mạng, giúp bảo vệ từng thiết bị lõi, vùng biên và thiết bị máy khách, dựa trên ba nhân tố chính: Xác thực danh tính những người truy nhập mạng, quy trình kiểm soát và công nghệ được áp dụng để bảo vệ những nội dung trên.

Hai mục tiêu đầu tiên có thể được hoàn thành với việc kiểm tra bảo mật thông thường, trong đó xác định những người có liên quan tới việc vận hành và chỉ rõ quyền bảo mật để thực thi các nhiệm vụ nhất định. Việc bảo vệ lõi mạng của máy chủ ứng dụng và các thiết bị tương tự như việc

bảo vệ mạng LAN trước những nguy cơ tấn công IP đã được biết đến như hack lỗ hổng hệ điều hành (OS vulnerabily), tấn công từ chối dịch vụ/từ chối dịch vụ phân tán (DOS/DDOS), hoặc các dạng xâm nhập trái phép khác.

Đối với bất cứ một hệ điều hành nào cũng cần sử dụng phiên bản mới nhất với tất cả bản vá lỗi đã được cài đặt và bỏ đi dịch vụ không rõ nguồn gốc cũng như tài khoản người dùng để kiểm soát truy cập từ xa.

Hãng bảo mật Mỹ khuyến cáo các doanh nghiệp cân nhắc việc sử dụng những hệ thống phòng ngừa và phát hiện xâm nhập trái phép (IDP/IPS) để kiểm soát lưu lượng. Một hệ thống như thế có thể gói tới lớp 7 để xác định những đe dọa tiềm ẩn. Chẳng hạn như, mục tiêu ưa thích của cuộc tấn công bằng sâu máy tính là một ứng dụng VoIP với giao diện web cho người quản trị và máy chủ web. Một thiết bị IDP có thể sử dụng nhiều phương thức để phát hiện sự khiêu khích và ngăn chặn những lưu lượng có hại bằng cách giảm các gói tin từ mạng.

Hàng loạt triển khai gateway cũng có thể được thấy ở lớp vùng biên. Thông thường, server cung cấp đăng ký người dùng, xác định lưu lượng VoIP đi vào và chuyển các cuộc gọi tới nơi đến. Hai giao thức chính cho lưu lượng VoIP là H.323 và SIP. Cả hai đều dùng giao thức truyền thời gian thực (Real-time Transport Protocol - RTP) cho truyền thông. Ứng dụng VoIP sẽ bắt đầu một phiên sử dụng cổng tĩnh để truyền thông tin và sau đó bắt đầu chuyển thông tin sử dụng một cổng ngẫu nhiên. Tuy nhiên, cho phép các kết nối tới một cổng bất kỳ là một mạo hiểm về bảo mật đối với những cuộc tấn công có chủ ý. Trong trường hợp như vậy, nên có một gateway đặt phía sau một ứng dụng tường lửa bảo vệ VoIP (như dòng sản phẩm tường lửa tích hợp NetScreen). Các thiết bị firewall thông lượng cao cũng rất nên được xem xét, vì độ trễ của mạng sẽ ảnh hưởng tới chất lượng cuộc gọi.

Tường lửa cần cung cấp một cổng cấp độ ứng dụng để ngăn chặn lưu lượng VoIP, phân loại giao thức và kiểm tra những cổng động nào cần được mở bằng ứng dụng. Tính năng này mở một lối đi cho phép truyền thông tin trong một phiên thoại cụ thể và đóng lại sau khi hoàn thành cuộc gọi.

Khi người dùng kết thúc cuộc gọi qua IP thì nội dung đàm thoại đó vẫn là dữ liệu nhạy cảm, những thông tin này nhất thiết không được để lộ ra mạng công cộng. Do vậy, thiết bị điện thoại IP nên hỗ trợ cơ chế xác thực hiệu quả cho việc đăng ký đối với máy chủ VoIP. Việc mã hoá bổ sung với việc sử dụng một kênh mạng riêng ảo (VPN) cũng nên được áp dụng cho cả việc thiết lập cuộc gọi và truyền tải thông tin.

Tóm lại, công nghệ VoIP cung cấp cho doanh nghiệp những phương thức mới để tiết kiệm chi phí và nâng cao hiệu quả hoạt động. Để phát huy tối đa hiệu quả của công nghệ này, người quản trị nên dùng cách tiếp cận phòng vệ theo lớp để nắm rõ những mối đe doạ mạng và bảo đảm có thể chống lại những tấn công.

Xuân Kim