Tiêu đề: Kiểm soát nguy cơ tấn công mạng
Tác giả: Robert Trọng Trần - Giám đốc Dịch vụ An ninh mạng và Bảo mật thông tin, PwC Việt Nam
Nguồn: Thời báo Kinh tế Sài Gòn đăng ngày 20/05/2017
Đường dẫn bài viết: http://www.thesaigontimes.vn/160157/Kiem-soat-nguy-co-tan-cong-mang.html

Kiểm soát nguy cơ tấn công mạng

Robert Trọng Trần (*)
Thứ Bảy, 20/5/2017, 15:59 (GMT+7)

Chia sẻ:

(TBKTSG) - Vụ mã độc tống tiền tấn công vào các hệ thống máy tính ở gần 100 quốc gia và vùng lãnh thổ vào cuối tuần qua đã làm dấy lên mối lo ngại rủi ro an ninh ở thời đại Internet vạn vật kết nối.

Năm ngoái, thế giới đã chứng kiến những vụ tấn công từ chối dịch vụ (DDoS) với quy mô lớn chưa từng có, gây ra bởi mạng lưới các thiết bị kết nối Internet bị cài mã độc do tin tặc chiếm quyền điều khiển (botnet). Đây rõ ràng là hồi chuông cảnh báo doanh nghiệp cần nghiêm túc xem xét khả năng bảo mật của mình, ở thời đại Internet vạn vật kết nối (IoT) trở nên ngày càng phổ biến, và tin tặc ngày càng nắm trong tay nhiều công cụ để tấn công một cách có hệ thống. Thay vì e ngại và nghi ngờ điều này, doanh nghiệp hoàn toàn có thể chủ động thực hiện các biện pháp phòng ngừa, kiểm soát rủi ro để giành thế chủ động.

Với việc chiếm quyền điều khiển hàng loạt những thiết bị công nghệ bảo mật kém như máy in, máy quay phim hay bộ định tuyến (router) với số lượng lớn, tin tặc ngày nay cho thấy chúng hoàn toàn đủ khả năng phát động những vụ tấn công quy mô lớn hơn nữa thông qua mạng lưới các botnet. Dyn, nhà cung cấp kết nối Internet bị tấn công DDoS hồi năm ngoái dẫn đến việc hàng loạt trang web lớn ở châu Âu và Bắc Mỹ không thể truy cập được trong nhiều giờ liền, cho biết họ đã bị tấn công bởi một mạng lưới botnet lên đến 100.000 thiết bị dính mã độc Mirai. Vụ tấn công này nghiêm trọng đến mức một hãng sản xuất hàng điện tử có ý định thu hồi sản phẩm để vá lỗ hổng bảo mật. Nó cũng được đánh giá là vụ tấn công DDoS quy mô lớn nhất từ trước đến nay.

Có thể nói, mối nguy tấn công mạng thông qua các thiết bị IoT sẽ không ngừng gia tăng và có thể gây ra hậu quả nghiêm trọng hơn. Doanh nghiệp rõ ràng sẽ cần phải chuẩn bị cho viễn cảnh bị tấn công thường xuyên hơn bởi tin tặc không chuyên nhưng được trang bị những công cụ tối tân. Khảo sát "Thực trạng an toàn thông tin toàn cầu 2017" do PwC thực hiện cho thấy thời gian trung bình doanh nghiệp phải tạm dừng hoạt động từ một cuộc tấn công mạng là 20,2 giờ/năm. Con số này đã gia tăng không ngừng trong những năm qua, nhưng doanh nghiệp có thể khái quát hóa các rủi ro an ninh từ Internet vạn vật để có thể bảo vệ tài sản hiệu quả hơn.

Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Tiêu đề: Kiểm soát nguy cơ tấn công mạng
Tác giả: Robert Trọng Trần - Giám đốc Dịch vụ An ninh mạng và Bảo mật thông tin, PwC Việt Nam
Nguồn: Thời báo Kinh tế Sài Gòn đăng ngày 20/05/2017
Đường dẫn bài viết: http://www.thesaigontimes.vn/160157/Kiem-soat-nguy-co-tan-cong-mang.html

Củng cố khả năng hồi phục

Trước tiên, doanh nghiệp cần chú trọng nâng cao khả năng khôi phục hoạt động sau khi bị tấn công như sử dụng cùng lúc nhiều nhà cung cấp máy chủ DNS khác nhau. Việc lập sẵn kế hoạch khôi phục sau khi bị tấn công cũng giúp doanh nghiệp nhanh chóng hồi phục trong trường hợp xấu nhất như khi bị tin tặc sử dụng botnet để tấn công DDoS làm cản trở hoạt động kinh doanh, hoặc tấn công trực tiếp vào các thiết bị của doanh nghiệp để đánh cắp thông tin. Trong bối cảnh Internet vạn vật càng trở nên phổ biến, việc sao lưu dữ liệu, hướng dẫn nhân viên cách phòng ngừa tin tặc và lập sẵn kế hoạch cho tình huống xấu nhất phải được doanh nghiệp thực hiện càng sớm càng tốt. Các doanh nghiệp có chiến lược an ninh mạng bài bản, hệ thống và được thực hiện một cách tự động sẽ có khả năng hồi phục, vượt qua mối nguy tin tặc hiệu quả hơn.

Đánh giá và kiểm soát các nguy cơ

Cấp lãnh đạo cần chú ý hơn đến các mối nguy tiềm ẩn liên quan đến IoT khi thảo luận chiến lược an ninh mạng cho doanh nghiệp. Thực tế, lãnh đạo các doanh nghiệp trên toàn cầu cũng đã bắt đầu quan tâm đến điều này. Khảo sát của PwC cho thấy có đến 46% người trả lời cho biết họ có kế hoạch đầu tư giải pháp bảo mật cho Internet vạn vật trong 12 tháng tới. Ngoài ra, có 35% người trả lời cho biết họ có sẵn kế hoạch bảo mật cho Internet vạn vật, và 28% đang thực thi một kế hoạch bảo mật cho Internet vạn vật.

Dù vậy, vẫn còn rất nhiều việc cần làm. Các tổ chức hoạt động dựa vào IoT, đặc biệt là ở những lĩnh thực thiết yếu, cần phải hiểu được quy mô của vấn đề và xem xét phân bổ chi phí nâng cấp khả năng bảo mật của tất cả các thiết bị IoT trong hệ thống sao cho hiệu quả. Điều này rất quan trọng, bởi tin tặc hiện đã có thể dò tìm được bất kỳ thiết bị nào có kết nối Internet. Ví dụ, nguy cơ ở lĩnh vực chăm sóc sức khỏe là khá nghiêm trọng, bởi hầu hết máy móc thiết bị y tế đều đã được kết nối vào Internet. Khảo sát của PwC cho thấy ở các nước phát triển, trung bình một phòng bệnh sẽ có từ 3-10 thiết bị có kết nối Internet.

Bảo mật các thiết bị IoT

Đối với các nhà sản xuất thiết bị kết nối Internet, việc cần làm ngay từ bây giờ là thiết kế sản phẩm với tư duy ưu tiên các tính năng bảo mật; cần thiết kế để người dùng có thể dễ dàng cập nhật các bản vá lỗ hổng bảo mật cho thiết bị một cách thuận tiện nhất. Nhà sản xuất không nên đặt mật khẩu mặc định cho các thiết bị mà người dùng không thể thay đổi được. Các thiết bị này cũng nên được tích hợp thêm tính năng lưu trữ thông tin truy cập, cho phép phát hiện các dấu hiệu thâm nhập bất hợp pháp. Ngoài ra, thiết bị IoT cũng phải được thiết kế để có thể hoạt động ổn định trong môi trường bất ổn và có thể dừng hoạt động một cách an toàn trong trường hợp bị cài mã

Chị Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 4 3946 2246, máy lẻ 4690, Email: vu.thi.thu.nguyet@vn.pwc.com

Tiêu đề: Kiểm soát nguy cơ tấn công mạng
Tác giả: Robert Trọng Trần - Giám đốc Dịch vụ An ninh mạng và Bảo mật thông tin, PwC Việt Nam
Nguồn: Thời báo Kinh tế Sài Gòn đăng ngày 20/05/2017
Đường dẫn bài viết: http://www.thesaigontimes.vn/160157/Kiem-soat-nguy-co-tan-cong-mang.html

độc. Việc thử nghiệm khả năng bảo mật trong quá trình phát triển thiết bị IoT cần phải được bắt buộc thực hiện. Thiết bị cần có tính năng yêu cầu người dùng đổi mật khẩu mặc định trong lần sử dụng đầu tiên để tránh bị tin tặc tấn công.

Tóm lại, không còn có thể xem thường nguy cơ mất an ninh ở thời đại Internet vạn vật. Doanh nghiệp cần hiểu rõ và đánh giá đúng mức nguy cơ bị tin tặc tấn công thông qua thiết bị, cần xem xét tất cả yếu tố bên trong lẫn bên ngoài, bởi trong bối cảnh Internet kết nối toàn cầu và không doanh nghiệp nào có thể hoạt động đơn lẻ, sẽ không có biện pháp bảo mật nào là toàn vẹn.

(*) Giám đốc, Dịch vụ An ninh mạng, PwC Việt Nam