Kỷ nguyên của IoT *(Ảnh minh họa).*

Cần thay đổi giải pháp bảo mật thông tin trong kỷ nguyên số?

Hồ Thị Hạnh
Học viện Kỹ thuật quân sự

Trong kỷ nguyên Internet kết nối vạn vật (IoT), tình hình an ninh thông tin có nhiều diễn biến phức tạp, với nhiều cuộc tấn công mạng quy mô lớn. Vấn đề an toàn, an ninh mạng đang dần mang thêm màu sắc chính trị, với sự gia tăng theo cấp số nhân của các mối đe dọa về mất an toàn thông tin, khiến các hệ thống bảo mật truyền thống không thể đáp ứng kịp. Vì vậy, sự thay đổi về giải pháp bảo mật thông tin trong tương lai là hết sức cần thiết.

Sự bùng nổ kết nối và những nguy cơ tiềm ẩn

Khái niệm về IoT đã được đưa ra từ năm 1999 nhưng xu hướng này mới chỉ được chú ý và thực sự bùng nổ trong những năm gần đây. Theo đó, có thể hiểu IoT là mạng lưới kết nối mọi vật với Internet có khả năng thu thập và trao đổi dữ liệu. Với những ưu điểm của mình, công nghệ IoT trở thành hạt nhân của cuộc cách mạng công nghiệp lần thứ 4 và là cơ sở tạo ra sự hội tụ giữa ứng dụng vật lý và ứng dụng kỹ thuật số. Sự phát triển của IoT không chỉ dẫn đến sự nhảy vọt về năng lực sản xuất của các doanh nghiệp mà còn góp phần quan trọng trong việc đem đến cho người dùng những sản phẩm, dịch vụ chưa từng có từ trước tới nay.

Có 2 vấn đề chính được nêu ra

trong kỷ nguyên IoT. Đầu tiên là số lượng của các thiết bị kết nối đang bùng nổ. Theo báo cáo của Gatner (Hoa Kỳ) - Công ty nghiên cứu và tư vấn về công nghệ thông tin hàng đầu thế giới, trong năm 2016, số lượng thiết bị kết nối trong hệ thống IoT trên toàn cầu là 6,5 tỷ, tăng hơn 30% so với năm 2015, ước tính đến năm 2020 số lượng thiết bị kết nối không dây hoạt động sẽ vượt quá 30 tỷ. Như vậy, chỉ cần chiếm được một phần nhỏ thiết bị này cũng đủ để cho tội phạm mạng gây ra những vụ tấn công kinh hoàng nhất từ trước tới giờ và thu về những khoản lợi phi pháp khổng lồ. Thứ hai là, một số thiết bị kết nối có chứa dữ liệu cá nhân, thông tin về các hoạt động vận hành cũng như dữ liệu bí mật của doanh nghiệp, nên rất nguy hiểm cho cá nhân/ doanh nghiệp nếu bị tin tặc tấn công và sao chép. Theo Forrester Research (công ty nghiên cứu thị trường hàng đầu của Hoa Kỳ), sự an toàn của IoT đang trong "giai đoạn sáng tạo" nên không có các tiêu chuẩn hoặc sự kiểm soát về chất lượng. Còn theo Giám đốc nghiên cứu về an toàn thông tin của Công ty Nghiên cứu thị trường 451 Research (Hoa Kỳ), để đưa ra sản phẩm với mức giá phải chăng, hướng đến số đông khách hàng, các nhà sản xuất thường lơ là trong việc tích hợp giải pháp bảo mật mạnh vào các thiết bị và hệ thống của mình.

Năm 2016, cuộc tấn công mạng vào Dyn - Nhà cung cấp dịch vụ phân giải tên miền (DNS) của Hoa Kỳ đã gây hậu quả nghiêm trọng. Đây là lần đầu tiên trong một chiến dịch quy mô lớn, những kẻ tấn công không trực tiếp đánh sập máy chủ. Thay vào đó, chúng kích hoạt phần mềm độc hại Mirai vào các dịch vụ nhằm tự động phát hiện ra các thiết bị trong hệ thống IoT và chiếm quyền điều khiển các thiết bị bảo mật kém, cho phép kẻ tấn công kết nối khoảng 100.000 thiết bị không an toàn này vào một botnet được kiểm soát tập trung. Sau đó, tin tặc tung ra một cuộc tấn công từ chối dịch vụ (DDoS) vào các máy chủ của Dyn. Dyn phục vụ nhiều khách hàng lớn như Amazon, Etsy, GitHub, Shopify, Twitter…, nên khi các máy chủ của công ty không thể phân giải tên miền cho các khách hàng của mình, rất nhiều người không truy cập được vào các trang này, tạo cảm tưởng mạng Internet bị đánh sập.

Theo công bố của IBM, cơ sở dữ liệu IBM X-Force® đã ghi nhận 96.000 lỗ hổng bảo mật, trong đó chỉ riêng năm 2015 có 8.956 vụ, với thiệt hại trung bình gây ra cho mỗi doanh nghiệp lên đến 4 triệu USD. Tội phạm mạng và những mối đe dọa an ninh mạng đang gia tăng nhanh chóng, gây thiệt hại cho nền kinh tế toàn cầu từ 375 đến 575 tỷ USD/năm; điểm đặc biệt là không có khu vực địa lý hay ngành nghề, lĩnh vực nào được coi là miễn nhiễm.

Theo kết quả khảo sát mới nhất của IBM, trong nội dung "An ninh mạng trong kỷ nguyên nhận thức" được thực hiện với 700 giám đốc an ninh thông tin (CISO) và các nhà lãnh đạo an ninh khác đến từ 35 quốc gia cho thấy, sự gia tăng lớn trong chi phí về an ninh mạng. Hơn 70% người được hỏi cho biết, chi phí cho an ninh không gian mạng chiếm từ 10 đến 15% ngân sách dành cho công nghệ thông tin. Còn trong báo cáo "Bảo mật công nghệ thông tin" của Kaspersky Lab - Hãng sản xuất và phân phối phần mềm bảo mật số 1 của Nga và Công ty Nghiên cứu thị trường kinh nghiệm nhất trên thế giới B2B International đã chỉ ra rằng, chi phí khắc phục một sự cố an ninh mạng đang tăng lên, từ vài nghìn (trước đây) lên đến vài chục nghìn, thậm chí hàng trăm nghìn USD. Cụ thể, năm 2017 các doanh nghiệp vừa và nhỏ đã chi trả trung bình 87.800 USD cho mỗi sự cố bảo mật, trong khi các doanh nghiệp lớn phải chi 992.000 USD; riêng đối với những tổ chức công nghiệp, việc đảm bảo an toàn thông tin thiếu hiệu quả gây thiệt hại lên tới 497.000 USD/năm. Vì vậy, cả các tập đoàn lớn cũng như các doanh nghiệp rất nhỏ (có tiềm lực tài chính yếu) đang bắt đầu xem việc đầu tư cho vấn đề an toàn, an ninh thông tin như một khoản đầu tư chiến lược (chiếm 1/4 ngân sách dành cho công nghệ thông tin).

Cần xu hướng bảo mật mới cho một kỷ nguyên đầy thách thức

Mặc dù thường đi kèm với những rủi ro cao về bảo mật, nhưng làn sóng phát triển của IoT là không thể ngăn cản. Theo cảnh báo của IBM, trạng thái an ninh không gian mạng đang đạt

đến điểm tới hạn, số lượng rủi ro về an ninh mạng đang gia tăng theo cấp số nhân. Mặc dù đội ngũ an ninh mạng vẫn đang nỗ lực để giải quyết vấn đề trước tình hình mới, nhưng các mối đe dọa thay đổi nhanh chóng, ngày càng chuyên nghiệp, biến tướng khó lường, khiến không thể nhận biết, phân loại và xử lý kịp thời bằng các phương pháp tiếp cận truyền thống.

Tất cả những thách thức, áp lực đối với nhà quản lý về an ninh mạng được cô đọng trong 3 vấn đề quan trọng: i) Phân tích thông tin tình báo; ii) Độ chính xác trong nhận biết; iii) Tốc độ phản ứng đối với các sự kiện an ninh mạng. Về yếu tố thứ nhất, trong sự kiện nêu trên của IBM, 65% số người được hỏi cho biết họ thiếu nguồn lực để phân tích các thông tin tình báo, 40% trả lời rằng việc nắm bắt được mối đe dọa và các lỗ hổng bảo mật mới là một thách thức đáng kể, chỉ 27% có sáng kiến để cải thiện vấn đề này trong vòng 2-3 năm tới. Khó khăn thứ hai là vấn đề nhận biết các thông báo chính xác (hiện đang có quá nhiều cảnh báo an ninh mạng bị sai), có đến 60% số người được hỏi cho rằng đang thiếu các nguồn lực để xác định, đánh giá mối đe dọa và nhận biết những sự kiện tiềm ẩn nào đang leo thang. Khi vẫn còn loay hoay để giải quyết 2 khó khăn trên, thì việc cải thiện tốc độ phản hồi, giúp xử lý nhanh các sự cố an ninh mạng còn rất xa vời.

Hầu hết các tổ chức vẫn đang nghiên cứu các sáng kiến khác nhau để cải thiện khả năng kiểm soát rủi ro về an ninh không gian mạng, nhưng vẫn chỉ tập trung vào những lựa chọn khá cơ bản, theo lối truyền thống (cải thiện hành vi của nhân viên thông qua các hoạt động nâng cao nhận thức về an toàn thông tin; triển khai phần mềm giám sát nhận dạng; cải thiện mạng, ứng dụng và bảo mật dữ liệu…). Chính việc tập hợp nhiều dữ liệu bảo mật, áp dụng nhiều khả năng phân tích, lại khiến khối lượng công việc đạt đến điểm tới hạn của những phương thức truyền thống. Theo nhận định của các chuyên gia, để giải quyết những yêu cầu về an toàn, an ninh thông tin trong kỷ nguyên số cần thiết lập được các hệ thống bảo mật biết nhận thức.

Về bản chất, hệ thống này được xây dựng trên cơ sở điện toán nhận thức - một công nghệ phân tích thông minh, có khả năng lựa chọn những thông tin hữu ích từ các kiến thức về an toàn thông tin từ trước đến nay (cả cấu trúc và phi cấu trúc) để đưa vào trung tâm dữ liệu phục vụ cho việc quản lý rủi ro bảo mật. Trong các cuộc tấn công nâng cao, tấn công có chủ đích APT (Advance Persistent Threat), tin tặc thường tạo lập một loại mã độc mới theo cơ chế custom-malware/zero-day dành riêng cho đối tượng bị tấn công do đã hiểu rõ AV/IPS của mục tiêu, nên dễ dàng phá vỡ các lớp phòng thủ. Nhờ công nghệ phân tích tăng cường (Augmented analytics), giải pháp bảo mật biết nhận thức cung cấp khả năng phát hiện rủi ro, hành vi đáng ngờ (behavior-based) theo thời gian thực và đưa ra các phản ứng kịp thời trước các cuộc tấn công. Giải pháp này cung cấp khả năng phát hiện tấn công nâng cao (IOA) dựa vào ứng dụng giám sát hành vi an toàn, giúp ngay lập tức phát hiện các hành vi đáng ngờ, bất thường xảy ra tại điểm cuối, đồng thời tự động sàng lọc, rồi đưa ra khuyến nghị hoặc ứng xử phù hợp. Có thể nói, hệ thống bảo mật biết nhận thức có khả năng "hiểu" được ngữ cảnh, hành vi và ý nghĩa của các luồng thông tin trên cơ sở phân tích dữ liệu cấu trúc và phi cấu trúc.

Hiện nay, ở các nước tiên tiến trên thế giới, chỉ có 7% các đơn vị triển khai giải pháp bảo mật biết nhận thức để cải thiện khả năng kiểm soát rủi ro về an ninh mạng, tuy nhiên với tình hình mất an toàn thông tin như hiện nay, số lượng này dự kiến sẽ sớm tăng lên gấp 3 lần trong một vài năm tới. Chúng ta sẽ sớm được chứng kiến sự hành động của các quốc gia, sự vào cuộc nghiêm túc của các tổ chức, doanh nghiệp nhằm nghiên cứu, triển khai rộng rãi giải pháp bảo mật biết nhận thức để nâng cao hệ thống "miễn dịch số" của họ trong kỷ nguyên của sự kết nối ✍