Đa dạng các giải pháp an ninh mạng cho doanh nghiệp

✧ HOÀNG MI

Trong bối cảnh an ninh mạng đang phải đối mặt với những thách thức to lớn từ các cuộc tấn công có chủ đích, hơn lúc nào hết, vấn đề an toàn và bảo mật hệ thống giữ vai trò vô cùng quan trọng và cấp thiết đối với nhiều tổ chức, đặc biệt là doanh nghiệp. Trước tình hình này, các chuyên gia đã đề xuất nhiều giải pháp an ninh mạng có thể ứng dụng tại Việt Nam nhằm góp phần giúp các doanh nghiệp, tổ chức nắm bắt và đánh giá các hiểm họa an toàn thông tin hiện hữu, cũng như ứng phó kịp thời trước sự phát triển nhanh chóng của các nguy cơ.

Khi mạng chưa thực sự an toàn

Ngày 02/11/2016, Cục An toàn thông tin (Bộ Thông tin và Truyền thông) thông báo về việc website tuyển dụng và tìm việc Vietnamworks bị tin tặc tấn công và có khả năng gây lộ thông tin cơ sở dữ liệu (CSDL) thành viên, bao gồm tên đăng nhập và mật khẩu đăng nhập (không mã hóa) để truy cập tài khoản Vietnamworks. Mặc dù ngay sau đó, đại diện Vietnamworks đã khẳng định *"toàn bộ những dữ liệu người tìm việc, nhà tuyển dụng và các cá nhân liên quan trên Vietnamworks đều được đảm bảo an toàn"*, thông tin về việc này vẫn khiến nhiều doanh nghiệp (DN) và người tìm việc lo ngại. Ngày 11/11/2016, ngân hàng Vietcombank cũng đã thông tin chính thức trên website nhằm khuyến cáo khách hàng của mình nếu đang là thành viên của Vietnamworks cần chủ động kiểm tra và thay đổi mật khẩu truy cập, nếu có sử dụng chung thông tin truy cập, để tránh rủi ro. Ngân hàng này cũng khuyến nghị không tiết lộ tên đăng nhập (username), mật khẩu truy cập/mã PIN của bất kỳ dịch vụ ngân hàng điện tử, mã OTP, số thẻ, số tài khoản cho bất cứ ai, qua bất kỳ kênh nào, như điện thoại, email, mạng xã hội, ứng dụng, website, đường link lạ… để đảm bảo an toàn cho các giao dịch ngân hàng trực tuyến. Điều đáng lưu ý là, trước đó không lâu, tin tặc cũng đã tấn công mạng của Vietnam Airlines tối 29/7/2016, gây hậu quả sân bay Nội Bài có hơn 30 chuyến, Tân Sơn Nhất có hơn 60 chuyến nội địa bị chậm từ 15 đến hơn 60 phút, do sau khi hệ thống thông tin bị tấn công, nhà chức trách đã tắt toàn bộ mạng nội bộ, và nhân viên phải làm thủ tục check-in bằng tay. Sau vụ việc này, Cục Hàng không Việt Nam đã phối hợp với Ủy ban An ninh hàng không dân dụng quốc gia chỉ đạo các cảng hàng không tăng cường an ninh, đặc biệt là các khu vực có màn hình, rà soát các khu vực nhạy cảm nhằm ngăn chặn sự việc tương tự.

An ninh mạng tại Việt Nam đang được đặt trong tình trạng báo động. Theo số liệu từ Trung tâm Ứng cứu khẩn cấp máy tính (Vncert), trong năm 2015, số sự cố tấn công mạng xảy ra tại Việt Nam là 31.585 lần. Trong nửa đầu năm 2016, con số này tăng gấp 4,4 lần. Ngoài ra, riêng trong năm 2015, đã có 62.863 dòng virus máy tính mới xuất hiện tại Việt Nam và 61,7

triệu lượt máy tính bị lây nhiễm. Trong đó, có 8.758 sự cố loại phishing (lừa đảo), 41.712 sự cố là deface (thay đổi giao diện trang web) và 77.160 sự cố dạng malware (tấn công bằng mã độc). Tuy vậy, không phải rủi ro nào cũng đến từ tin tặc bên ngoài. Kết quả nghiên cứu từ hãng công nghệ Symantec đã chỉ ra rằng, 59% nhân viên nghỉ việc hoặc bị đề nghị thôi việc đã ăn trộm dữ liệu, dù 79% trong số đó biết họ không được phép, và cũng chỉ 15% các tổ chức tiến hành kiểm tra lại các văn bản bị đánh cắp. Nếu như tội phạm mạng gây thiệt hại cho nền kinh tế toàn cầu khoảng 445 tỷ USD mỗi năm (theo nghiên cứu từ CSIS/McAfee) thì riêng tại Việt Nam, người dùng *"mất trắng"* 8.700 tỷ đồng hàng năm vì virus. Từ đó cho thấy, bất kỳ sự xâm nhập nào xuất phát từ bên ngoài hay bên trong tổ chức đều có thể gây ra những tổn hại to lớn, khó khắc phục, thậm chí có thể làm sụp đổ cả một *"đế chế"*.

Không chỉ Việt Nam, an ninh mạng cũng là mối quan ngại ở nhiều quốc gia trên thế giới. Sau một loạt các vụ tấn công mạng vào Bangladesh, Philippines, Đài Loan, Thái Lan và Việt Nam, theo các chuyên gia, mối lo ngại thực sự chính là ở châu Á. Một báo cáo của công ty an ninh mạng FireEye cho thấy, các tổ chức tại châu Á *"cho phép"* phần mềm độc hại *"cư ngụ trong hệ thống của họ"* trung bình 520 ngày trước khi phát hiện ra chúng, so với mức trung bình 146 ngày của thế giới. Công bố của tổ chức Osterman Research vào tháng 8/2016 cho thấy, trên thế giới có gần 500 nguy cơ mã độc mới phát sinh mỗi phút; hơn 2 triệu mẫu ransomware đã được phát hiện; trung bình mỗi giây có khoảng 19 thông tin định danh bị lấy cắp bởi

các hoạt động trực tuyến trên toàn thế giới; 1,5 tỉ định danh bị lộ năm 2015; tỉ lệ tấn công mạng tăng với tốc độ 47%; các vụ thâm nhập do mã độc tăng 259% trong 5 tháng gần đây, gây tổn thất, giảm doanh thu cho 1/3 các dịch vụ và ngừng hoạt động khoảng 20%.

Tìm kiếm giải pháp bảo vệ hệ thống mạng

Trước nguy cơ mất an toàn thông tin tại các tổ chức và DN, giới chuyên gia công nghệ cho rằng, với an ninh bảo mật, không phải đợi đến *"mất bò mới lo làm chuồng"*, nhiều DN đã và đang tìm kiếm, đầu tư một giải pháp bảo mật phù hợp nhằm bảo vệ tài sản và uy tín của chính mình.

Theo bà Nguyễn Ngọc Phương Mai, Phó Tổng giám đốc Công ty Lạc Việt, có rất nhiều nguy cơ đe dọa an ninh mạng, nhưng tập trung vào 5 nguyên do chính: tấn công từ trong nội bộ; đánh cắp dữ liệu; mã độc hóa dữ liệu; plug-in trình duyệt và lây nhiễm qua IoT (Internet of Things). Ngoài các nguy cơ tự nhiên (động đất, lũ lụt), xã hội (chiến tranh, khủng bố) thì nguy cơ đối với an ninh mạng đang là vấn đề đau đầu của những người quản lý các hệ thống thông tin. Vì vậy, cần có những công cụ và kỹ thuật tiên tiến hơn để bảo vệ lợi ích của các tổ chức, đảm bảo an toàn và duy trì kiểm soát được dữ liệu, bao gồm các thông tin nhạy cảm và tài sản trí tuệ. Một khi có thay đổi về hạ tầng kỹ thuật, thay đổi về nghiệp vụ, các DN và tổ chức sẽ phát sinh nguồn dữ liệu khổng lồ cần bảo vệ, phân tích và xử lý.

Trước những nguy cơ có thật nhưng lại thoắt ẩn thoắt hiện, gây nên nhiều thiệt hại cho DN, ông Trịnh Công Tâm, chuyên gia đến từ DellEMC cho rằng, những con số đáng báo động trên là hồi chuông mà người lãnh đạo và quản lý IT phải suy nghĩ. *"Rất nhiều giải pháp tạm thời được DN đưa ra, thậm chí có DN, tổ chức còn cấm nhân viên không được truy cập Facebook hoặc các mạng xã hội khác. Đây là một trong những cách cấm người dùng truy cập ra bên ngoài, nhằm không ảnh hưởng đến an ninh mạng của tổ chức. Nhưng điều đó không thể và không nên là giải pháp lâu dài"*, ông cho biết thêm. Cũng theo ông Tâm, mô hình an ninh 3 lớp chưa thực

Ông Trịnh Công Tâm, chuyên gia của DellEMC giới thiệu các giải pháp an ninh mạng tại hội thảo "Tăng cường an ninh mạng: Hiểm họa và giải pháp"

Bà Nguyễn Ngọc Phương Mai, Phó Tổng giám đốc Công ty Lạc Việt, chia sẻ các nguy cơ đe dọa an ninh mạng.

sự đáp ứng cho nhu cầu hiện tại. Với những DN phát triển nhanh và mạnh, khi hệ thống tăng trưởng thì dữ liệu cũng tăng theo, nhưng các tiện ích lại chưa đáp ứng được. Ngoài chi phí đáng kể cho thiết bị IT và nhân sự khi phát triển hệ thống, mô hình kiến trúc mạng truyền thống không đảm bảo được an toàn an ninh mạng cho DN, đặc biệt là khi sự cố hệ thống xảy ra. Những lúc này, việc ảo hóa chính là giải pháp cho các trung tâm dữ liệu thế hệ mới.

Ông Hoàng Văn Thắng, chuyên gia tư vấn giải pháp hệ thống của Lạc Việt, cho biết: *"Hiện tại chưa có một hệ thống thông tin nào có thể đảm bảo an toàn tuyệt đối trước các cuộc tấn công mạng, nên việc chuẩn bị nhằm hạn chế rủi ro và ứng cứu sự cố phải được đặt lên hàng đầu. Những hậu quả nghiêm trọng mà các tổ chức phải gánh chịu từ các cuộc đột kích có chủ đích trong thời gian qua chính là hồi chuông cảnh tỉnh cho vấn đề bảo mật và an toàn thông tin trong DN"*. Từ kinh nghiệm thực tiễn trong việc triển khai các giải pháp an ninh mạng cho nhiều DN, theo ông có 7 giải pháp có thể xây dựng và vận hành một hệ thống an ninh mạng hiệu quả cho tổ chức, DN.

"Thời điểm này, các DN cần có biện pháp theo dõi, phân tích, phản ứng và xử lý kịp thời các sự cố, dù là nhỏ nhất. Nguy cơ an toàn thông tin không phải ở đâu xa, mà đang rất gần, gần đến mức chúng ta có thể cảm nhận được", theo ông Đỗ Đức Huy, chuyên gia tư vấn giải pháp công nghệ của RSA/DellEMC. Trong bất kỳ tình huống nào, đòi hỏi vẫn là phải đảm bảo được môi trường làm việc linh hoạt, vẫn nâng cao hiệu quả kinh doanh, khả năng ứng biến và tốc độ tăng trưởng của tổ chức. Theo ông, các DN nên xây dựng *"Trung tâm bảo mật"* của chính mình, ngay tại DN mình để có thể theo dõi, phát hiện và ứng cứu kịp thời khi các nguy cơ xảy ra. Đây là sự tổng hòa giữa con người, các quy trình và giải pháp công nghệ. Sau khi ảo hóa, các giải pháp công nghệ có thể giúp quản lý sự kiện bảo mật tập trung, theo dõi, điều tra và truy vết dữ liệu mạng, theo dõi và điều tra trên thiết bị đầu cuối. Điều này sẽ ngăn chặn đáng kể thời gian để cho kẻ tấn công đạt được các mục tiêu thâm nhập và gây thiệt hại cho hệ thống thông tin và nghiệp vụ. ❑