Tiêu đề: Doanh nghiệp ần đầu tư nhiều cho an toàn thông tin
Tác giả: Hoàng Thu
Nguồn: Thời Báo Kinh Tế Việt Nam, xuất bản ngày 08/06/2018

Doanh nghiệp cần đầu tư nhiều cho an toàn thông tin

Nhiều lãnh đạo doanh nghiệp (DN) tại Việt Nam vẫn coi an toàn thông tin là việc của bộ phận IT. Chia sẻ với TBKTVN, ông Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng và Bảo mật của PwC Việt Nam cho rằng, tư duy này cần thay đổi bởi khi tấn công mạng xảy ra, uy tín và kết quả kinh doanh của DN sẽ bị ảnh hưởng nghiêm trọng.

HOÀNG THU

Ông Robert Trọng Trần

Robert Trọng Trần bắt đầu sự nghiệp tại Solsoft (giờ là Infoblox) – nơi ông có cơ hội làm việc với nhiều chuyên gia đẳng cấp thế giới về an ninh mạng như nhà sáng lập của Nessus và Qualys. Trước khi về với PwC Việt Nam, ông Robert là chuyên gia tư vấn cấp cao về an ninh mạng tại GE Capital, Safran Morpho, Cap Gemini và nhiều công ty đa quốc gia khác tại Pháp và Anh.

Ông đánh giá như thế nào về thực trạng các cuộc tấn công mạng vào các DN Việt Nam trong thời gian gần đây? Có sự khác biệt nào đáng kể giữa xu hướng của các cuộc tấn công mạng hiện nay so với trước đây, thưa ông?

Các cuộc tấn công mạng vào các DN Việt Nam trong thời gian qua có xu hướng gia tăng cả về số lượng và mức độ ngày càng tinh vi. Trước kia, hacker sau khi xâm nhập vào hệ thống sẽ tìm cách xóa dữ liệu hoặc thay đổi giao diện của website thì ngày nay hacker sẽ tìm cách làm sao để đi sâu vào hệ thống để lấy được những dữ liệu quan trọng. Đặc biệt các cuộc tấn công ngày xưa thường là tự phát bởi các tổ chức hacker tên tuổi thì ngày nay đứng sau các cuộc tấn công được hậu thuẫn bởi các chính phủ hay tổ chức lớn. Mục đích của các cuộc tấn công mạng này là đánh cắp các thông tin liên quan đến sở hữu trí tuệ, tài chính. Mục tiêu yêu thích mà hacker nhắm đến là các ngân hàng, DN và tổ chức về bảo hiểm, ngành công nghiệp trọng điểm quốc gia như hệ thống điều khiển điện, dầu khí.

Các DN Việt Nam ngày càng trở thành mục tiêu tấn công của các hacker không chỉ ở trong nước mà trên thế giới. Lí do là sự phát triển của Việt Nam về an toàn thông tin còn rất thấp so với các nước vì vậy DN Việt Nam trở thành mục tiêu dễ dàng cho các cuộc tấn công mạng.

Theo ông, đâu là những nguyên nhân chính khiến an toàn thông tin của Việt Nam vẫn ở mức thấp như vậy?

Đầu tiên phải kể đến sự hiểu biết về an toàn thông tin của các DN Việt Nam vẫn khá thấp. Một trong những suy nghĩ sai lầm thường thấy là DN mình còn nhỏ nên chưa phải là mục tiêu tấn công của các hacker. Nhưng thực tế không phải như vậy. Đơn cử, các ngân hàng lớn trên thế giới như HSBC Hồng Kông thường đầu tư hàng trăm triệu USD cho hệ thống an toàn thông tin. Vì vậy, hacker không dễ để đột nhập vào những DN hay tổ chức lớn như vậy. Thay vào đó, DN nhỏ với hệ thống phòng vệ lỏng lẻo lại trở thành mục tiêu bị tấn công.

Như ông vừa đề cập, các DN và tổ chức lớn có thể chi một khoản không nhỏ để đầu tư cho an toàn thông tin. Nhưng chi phí đầu tư vẫn luôn là một câu chuyện "đau đầu" với các DN vừa và nhỏ tại Việt Nam, thưa ông?

Chi phí mà DN rót vào để cải thiện an toàn thông tin sẽ không phải là khoản đầu tư mất đi. DN đầu tư vào an toàn thông tin giống như một cách giúp đưa "brand" (thương hiệu) của họ lên một tầm cao hơn. Khi đầu tư vào an toàn thông tin, DN sẽ có rất nhiều cái lợi và các khoản đầu tư này sẽ mang lại giá trị xét về lâu dài.

Ông có đề xuất và lời khuyên gì dành cho các DN Việt Nam khi đầu tư cho an toàn thông tin trong thời gian tới?

DN cần hiểu tình trạng hiện tại mình đang như thế nào, những gì họ đang có là quan trọng nhất. Sau khi đánh giá được tổng thể hiện trạng thì cần có chiến lược và kỳ vọng cụ thể về mức độ an toàn thông tin đạt được sẽ đến đâu để ra quyết định đầu tư. Đầu tư mà không có chiến lược rõ ràng thì giống như mang tiền bạc đổ xuống sông, xuống biển.

Có một sai lầm mà nhiều DN Việt Nam mắc phải là mua các máy móc rất đắt tiền về mà không biết dùng. Trên thực tế, kỹ thuật chỉ là một phần nhỏ trong an toàn thông tin. Đầu tư vào an toàn thông tin thì quan trọng nhất là con người.

Ở Việt Nam, các bạn trẻ có khả năng học hỏi khá nhanh nhạy và tôi tin rằng nếu được đào tạo bài bản sẽ có kết quả tốt. Tôi đã thấy có DN Việt Nam thực hiện chiến lược cải thiện an toàn thông tin bằng việc đưa các khóa đào tạo về vấn đề này cho toàn bộ nhân viên. Trong quá trình đào tạo, nếu nhân viên nào đạt điểm quá thấp thì sẽ bị hạ lương. Tôi cho rằng mô hình này rất hay và hiệu quả mà lại không quá khó để áp dụng.

Vũ Thị Thu Nguyệt, Trưởng phòng Truyền thông và Marketing, ĐT: +84 24 3946 2246 Máy lẻ: 4690, Email: vu.thi.thu.nguyet@pwc.com