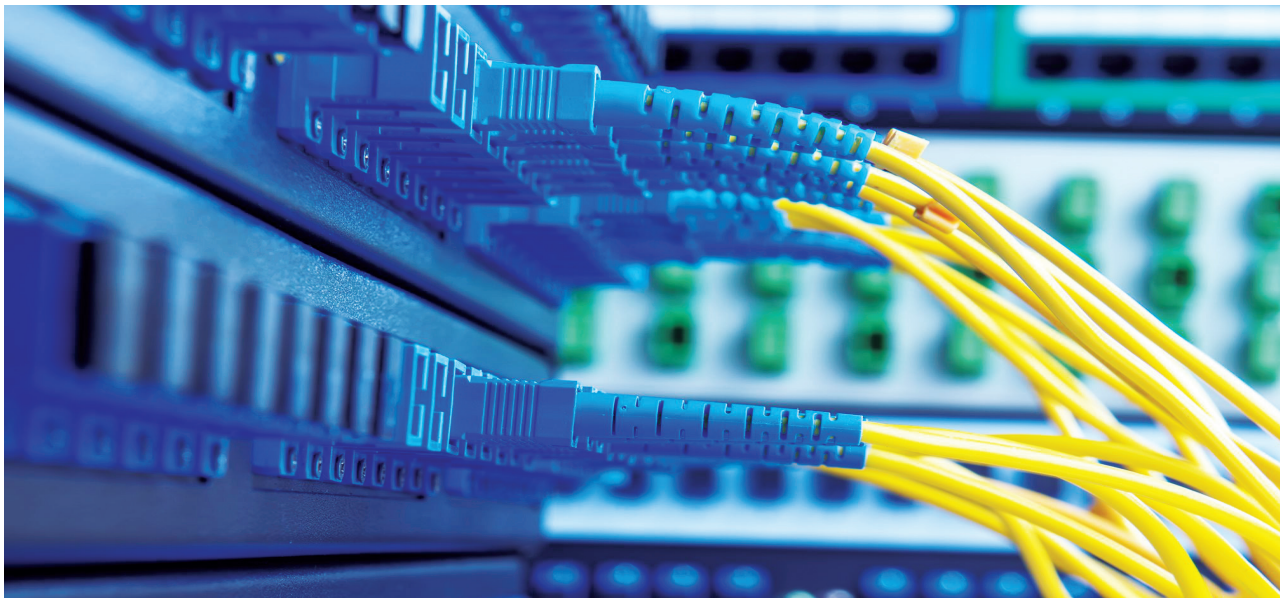
Tiêu đề: Lỗ hổng bảo mật từ đối tác
Tác giả: Huy Vũ
Nguồn: Nhịp cầu Đầu tư, xuất bản ngày 12/12/2016

Huy Vũ

LỖ HỔNG BẢO MẬT TỪ ĐỐI TÁC



Ảnh: vn.123rf.com

Việt Nam có nguy cơ cao trở thành "cổng sau" của tin tặc để tấn công vào các công ty toàn cầu.

NĂM 2013, TIN TẶC ĐÃ TẤN CÔNG VÀO CHUỖI CỬA HÀNG BÁN LẺ TARGET (MỸ) và lấy đi thông tin về thẻ tín dụng và thẻ tài khoản của 40 triệu khách hàng. Tuy nhiên, ít ai biết rằng thủ phạm không tấn công trực tiếp vào trụ sở chính của Target mà nhắm vào các đối tác của họ, nơi có chính sách bảo mật kém hơn, rồi từ đó chiếm quyền kiểm soát hệ thống Target.

Kịch bản này được cho là sẽ tái diễn với tần suất nhiều hơn ở ngành công nghiệp sản xuất trong thời gian tới, đặc biệt là khi công ty ở các quốc gia phát triển mở rộng mạng lưới đối tác ở những nước đang phát triển. Theo báo cáo toàn cầu công bố năm 2015 của Tổ chức Repository of Industrial Security Incidents (RISI), giới tin tặc đang chuyển hướng tấn công vào khu vực sản xuất. Các ngành như năng lượng, dầu khí, vận tải hành khách, quản lý nước và chất thải, đồ ăn, hóa chất, điện tử và các công ty gia công là những mục tiêu ưa thích.

Lý do rất đơn giản: khả năng tự vệ trước tội phạm mạng của nhóm này rất yếu. Theo khảo sát của RISI, đa phần giám đốc điều hành nhà máy, nhất là nhà máy nhỏ và vừa, đều cho rằng công ty của họ không chứa dữ liệu cá nhân nên không thể là mục tiêu tấn công hấp dẫn. Việc phòng chống cũng vì thế mà lỏng lẻo.

Theo ông Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng của PwC Việt Nam, giống như trường hợp Target, tin tặc sẽ không tấn công trực tiếp vào công ty đứng đầu chuỗi cung ứng, thường đầu tư rất lớn cho công tác bảo mật do việc xâm nhập sẽ tốn thời gian và khó khăn hơn. Thay vào đó, nhóm này sẽ tấn công vào các đối tác nằm trong chuỗi cung ứng ở những quốc gia đang phát triển. Khi đã nắm quyền kiểm soát, tin tặc sẽ bắt đầu phát tán mã độc gián điệp đến các công ty mục tiêu. Một trong những hình thức phổ biến nhất là gửi email về chứng từ thanh toán kèm mã độc đến kế toán.

Trên thực tế, đã từng có vài trường hợp xảy ra ở Việt Nam. Ông Võ Đỗ Thắng, Giám đốc Trung tâm An ninh mạng Athena, cho biết, năm 2009, một công ty sản xuất cơ khí chính xác cho ngành hàng không, ôtô ở Bình Dương đã bị đánh cắp toàn bộ dữ liệu thiết kế các sản phẩm được gửi từ công ty mẹ ở Mỹ. Nguyên nhân là do mã độc đã được cài vào máy chủ của Công ty ở Việt Nam. Bên cạnh đó, do ý thức bảo mật kém, các doanh nghiệp sản xuất cũng rất dễ bị đối thủ cạnh tranh lợi dụng tội phạm mạng làm gián đoạn kinh doanh hoặc gây thiệt hại tài sản.

Theo khảo sát của Allianz Global Corporate & Specialty với 500 nhà quản lý rủi ro ở 47 quốc gia, giá trị trung bình của một vụ tấn công

Tiêu đề: Lỗ hổng bảo mật từ đối tác
Tác giả: Huy Vũ
Nguồn: Nhịp cầu Đầu tư, xuất bản ngày 12/12/2016

gây gián đoạn công việc kinh doanh vào khoảng 1,6 triệu USD. Còn cuộc tấn công vào nhà máy sản xuất thép ở Đức vào năm 2014, gây tê liệt nhiều dây chuyền sản xuất đã làm thiệt hại về vật chất khoảng 50 triệu USD.

Theo ông Robert Trọng Trần, dù rơi vào trường hợp nào đi nữa, các chính sách bảo mật kém sẽ gây khó cho doanh nghiệp sản xuất trong nước trong việc hợp tác với đối tác nước ngoài. Nhất là sau hàng loạt vụ tấn công vừa qua, các công ty toàn cầu đã bắt đầu quan tâm đến khả năng tự bảo vệ của các đối tác trước tội phạm mạng. Điển hình như GE Capital (Mỹ) yêu cầu đối tác phải có hợp đồng bảo hiểm an ninh mạng. Xu hướng này được dự đoán sẽ phổ biến trong thời gian tới.

Báo cáo của hãng bảo mật Kaspersky và Symantec năm ngoái cho biết, Việt Nam đứng thứ 3 thế giới về số người sử dụng điện thoại di động bị tấn công mạng, đứng thứ 12 trên thế giới về các hoạt động tấn công mạng. PwC Việt Nam ước tính, hằng năm Việt Nam thiệt hại khoảng 8.000 tỉ đồng vì tin tặc.

Theo Trung tâm Ứng cứu khẩn cấp máy tính (VNCERT), sự cố gồm cả sự cố lừa đảo (Phishing), tấn công thay đổi giao diện (Deface) và mã độc (Malware) 6 tháng đầu năm tăng lên chóng mặt, gấp 4,4 lần so với năm 2015. Mặc dù vậy, ý thức phòng chống tội phạm mạng của doanh nghiệp trong nước nói chung và doanh nghiệp sản xuất nói riêng, theo ông Thắng của Athena, là vẫn thờ ơ như chưa hề có các công bố nói trên. "Đa phần doanh nghiệp bị tấn công thấy rằng hoạt động của họ vẫn bình thường nên không quan tâm, đến khi sự cố xảy ra thì đã muộn", ông Thắng cho biết.

Hằng năm, ước tính Việt Nam thiệt hại khoảng 8.000 tỉ đồng vì tin tặc.

Theo tìm hiểu của NCĐT, một trong những nguyên nhân khiến doanh nghiệp sản xuất không muốn đầu tư cho bảo mật là do chi phí đầu tư cho hạ tầng, phần mềm khá tốn kém. Bên cạnh đó, nhân sự trong ngành bảo mật ở Việt Nam hiện khá mỏng và yếu.

Tuy nhiên, theo ông Thắng, chi phí cho việc bảo mật đã giảm đi đáng kể so với 10 năm trước nhờ vào công nghệ điện toán đám mây và các dịch vụ thuê ngoài nhân sự ngành bảo mật. Vì vậy, bảo mật yếu là do rất ít chủ doanh nghiệp xem công tác phòng chống bảo mật là một phần của việc quản trị rủi ro, cụ thể là bảo mật thông tin.

"Nguyên nhân chính vẫn do ý thức của các chủ doanh nghiệp. Tuy nhiên, khi nền kinh tế Việt Nam ngày càng mở cửa và các công ty sản xuất trong nước tham gia nhiều hơn vào chuỗi cung ứng toàn cầu thì việc thờ ơ với tội phạm mạng có thể sẽ khiến họ bỏ lỡ nhiều cơ hội kinh doanh trong thời gian tới", ông Robert Trọng Trần nói. NCĐT

Anh Nguyễn Ngọc Hà, Phó trưởng phòng Truyền thông và Marketing, ĐT: +84 8 3823 0796 Máy lẻ: 4692, Email: nguyen.ngoc.ha@vn.pwc.com