Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?

28/11/2016 16:58

(TBTCO) - Tội phạm mạng đang trở thành mối lo ngại cho toàn xã hội, nhất là trong lĩnh vực ngân hàng, khi ngày càng xảy ra nhiều vụ tiền của khách hàng trong tài khoản bỗng nhiên bị "bốc hơi" trong thời gian gần đây...

Ảnh TL minh họa

Để tìm hiểu về vấn đề này cũng như công tác an ninh mạng đối với các tổ chức, doanh nghiệp ở Việt Nam hiện nay, PV TBTO đã có cuộc phỏng vấn và trao đổi với ông Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng, PwC Việt Nam.

PV: *Thưa ông, từ đầu năm tới nay ở Việt Nam đã xảy ra khá nhiều vụ việc khách hàng bị mất tiền trong tài khoản ngân hàng. Ông đánh giá thế nào thực trạng này?*

Ông Robert Trọng Trần: Theo thống kê của các hãng bảo mật trên thế giới, hầu hết những sự cố mất tiền kiểu như vậy điều xuất phát từ 2 nguyên nhân chính. Một là nhận thức về bảo mật của khách hàng khi sử dụng thẻ. Hai là các ngân hàng và đại lý bán hàng đã bị tin tặc tấn công trực tiếp, tuy nhiên tỷ lệ này rất thấp.

Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

Về nhận thức bảo mật, tôi tin rằng có không ít khách hàng ở Việt Nam đã bị tấn công phishing. Nghĩa là tin tặc đã gửi cho họ email chứa đường link giả mạo, giả dạng email từ ngân hàng, hoặc tạo các website bán hàng với giá bán cực kỳ hấp dẫn và yêu cầu khách hàng phải nhập thông tin thanh toán. Khi khách hàng nhập thông tin, mã pin... thì tất cả sẽ được chuyển về cho tin tặc. Thế là chúng có thể dễ dàng đánh cắp thông tin thẻ của nạn nhân từ đó thực hiện các giao dịch quan mạng.

Bên cạnh đó, một số tổ chức tội phạm đã mua máy in thẻ và in ra những thẻ tín dụng để thực hiện các giao dịch thẻ thường ngày. Hình thức này đã xuất hiện ở Việt Nam. Các giải pháp công nghệ bảo mật của ngân hàng sẽ không thể bảo vệ khách hàng trước các rủi ro này.

Còn đối với các ngân hàng Việt Nam, thực tế họ đã bắt đầu chú ý đến bảo mật và đã đầu tư giải pháp bảo mật tiên tiến của thế giới. Tuy nhiên, để nâng cao khả năng phòng chống, yếu tố cốt lõi đầu tiên là phải thay đổi tư duy của người lãnh đạo.

> *"Các tổ chức tài chính, ngân hàng thương mại nên nhìn nhận thật sự nghiêm túc mối nguy từ tin tặc, xem xét cân đối thêm ngân sách an ninh mạng nhằm tăng cường khả năng phát hiện/phản ứng và thiết lập thêm các biện pháp kiểm soát nhiều lớp bên trong hệ thống."*

Ông Robert Trọng Trần

Nhiều ngân hàng cho rằng bảo mật chỉ đơn giản là đầu tư hệ thống công nghệ mà quên đi yếu tố con người và quy trình. Đối với tin tặc chuyên nghiệp, chúng sẽ không tấn công trực diện vào hệ thống, mà nhắm vào yếu tố con người bên trong tổ chức. Thay vì tấn công trực tiếp vào hệ thống tường lửa, tin tặc có thể xâm nhập vào ngân hàng thông qua các cuộc tấn công lừa đảo.

Khi nhân viên ngân hàng đó mở tập tin nhiễm độc hay bấm vào liên kết giả mạo do chúng gửi đến, chúng có thể dễ dàng kiểm soát được những máy tính này và bắt đầu chiếm quyền hệ thống.

Ngoài ra, một vấn đề lớn khác khiến giới lãnh đạo ngân hàng đắn đo là ngân sách. Họ vẫn nhìn nhận an ninh mạng là gánh nặng chi phí, chứ không phải sự đầu tư cho tương lai. Họ cũng chưa đánh giá được các tác động đối với kinh doanh khi ngân hàng bị tấn công bởi tin tặc.

Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

PV: *Rõ ràng kinh phí luôn là một vấn đề đối với bất cứ ai, nhưng nếu có ngân sách để đầu tư cho an ninh mạng, thì theo ông nên đầu tư như thế nào?*

Ông Robert Trọng Trần: Có một thực tế là từ trước tới nay, phần lớn ngân sách dành cho công tác bảo mật, an ninh mạng đều được rót vào những công nghệ mang tính ngăn chặn như tường lửa, phần mềm diệt virus và các công nghệ chống xâm nhập khác. Còn khả năng phát hiện và phản ứng khi bị hệ thống xâm nhập thì lại chưa được các tổ chức quan tâm đầu tư đúng mức. Tuy nhiên, điều này đang có chiều hướng thay đổi khi các tổ chức chấp nhận thực tế rằng tin tặc có thể xâm nhập vào bất kì hệ thống nào.

Một khảo sát gần đây do Pierre Audoin Consultants (Anh) thực hiện trên 200 tổ chức tại Anh, Pháp và Đức cho thấy, khoảng cách giữa mức chi dành cho ngăn chặn xâm nhập và khâu phát hiện/phản ứng cũng đã được thu hẹp.

Với thực trạng trình độ an ninh mạng vẫn khá hạn chế của các tổ chức Việt Nam, rõ ràng đã đến lúc chúng ta cần chú trọng nhiều hơn đến khả năng phát hiện và phản ứng khi bị tin tặc xâm nhập, đồng thời đổi mới quy trình đánh giá mức độ bảo mật của hệ thống theo chuẩn hiện đại.

PV: *Tức là xu thế đầu tư cho an ninh mạng là "ngừng khóa cổng" để tăng cường "khóa cửa phòng"?*

Ông Robert Trọng Trần: Xu thế dịch chuyển trọng tâm đầu tư bạn nhắc đến không có nghĩa là chúng ta "ngừng khóa cổng". Sẽ không có chuyên gia nào khuyên doanh nghiệp dừng đầu tư vào các biện pháp chống tin tặc xâm nhập. Điều tôi nhìn thấy là chiến lược an ninh mạng đi vào chiều sâu, tăng cường khả năng phát hiện/phản ứng trước tin tặc đã được các doanh nghiệp bắt đầu quan tâm.

Đối với Việt Nam, tôi cảm thấy khả năng bảo mật của các doanh nghiệp, đặc biệt là các tổ chức tài chính là khá yếu và họ cũng gần như chưa có khả năng phát hiện dấu vết của tin tặc bên trong hệ thống. Tin tặc thậm chí có thể tự do di chuyển, tìm kiếm thông tin nhạy cảm của doanh nghiệp trong nhiều ngày mà không bị phát hiện. Vì thế, chúng ta phải biết một khi thâm nhập, hackers sẽ đi lại và tìm kiếm những thông tin nào. Từ đó mới có biện pháp ngăn chặn kịp thời, hoặc cản trở làm chậm bước tiến của chúng.

PV: *Không ít tổ chức tại Việt Nam vẫn đang thường xuyên thực hiện các bài kiểm tra đánh giá tình hình bảo mật mạng, nhưng sự cố liên quan đến tin tặc vẫn xảy ra. Vì sao lại như vậy? Liệu có giải pháp nào khác hay không?*

Ông Robert Trọng Trần: Kiểm tra và đánh giá tình hình bảo mật định kỳ chắc chắn sẽ giúp các tổ chức phòng chống tin tặc hiệu quả hơn. Nhưng vấn đề nằm ở chỗ các bài kiểm tra kiểu truyền thống chỉ thử nghiệm sức chống đỡ của hệ thống dựa trên những lỗi bảo mật đã được phát hiện.

Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

Không may là tin tặc chuyên nghiệp sẽ tấn công chúng ta thông qua những lỗi bảo mật chưa được ghi nhận (zero day bugs) và sẽ không thể bị các công cụ bảo mật như antivirus, firewall, IPS/IDS hay anti-APT ngăn chặn. Đây là lý do các tổ chức Việt Nam cần phải chuyển sang thực hiện các bài kiểm tra bảo mật mạng tiên tiến hơn càng sớm càng tốt.

Khác với cách kiểm tra truyền thống, công cụ mới dùng để đánh giá khả năng bảo mật sẽ mô phỏng một cuộc tấn công thực do tin tặc chuyên nghiệp thực hiện, thông qua những lỗi bảo mật chưa được ghi nhận. Trong vòng 24 giờ sau khi cuộc tấn công, lãnh đạo doanh nghiệp sẽ nhận được báo cáo rõ ràng và chi tiết về tình hình bảo mật hiện tại của hệ thống, tương quan với các doanh nghiệp cùng ngành, kèm theo hướng dẫn cụ thể về những hành động cần làm trong ngắn và dài hạn.

Cụ thể, công cụ đánh giá mới sẽ cung cấp cho các tổ chức hai thông tin quan trọng. Một là giúp họ biết tin tặc sẽ có thể đánh cắp hoặc kiểm soát dữ liệu nào sau khi xâm nhập vào hệ thống. Hai là cho họ biết hệ thống cảnh báo sẽ mất bao lâu để phát hiện hoạt động của tin tặc bên trong.

Những thông tin quan trọng này có thể giúp chúng ta thiết lập thêm các công cụ kiểm soát, ngăn chặn nhằm bảo vệ dữ liệu mật trong hệ thống, qua đó nâng cao khả năng phát hiện/phản ứng. Dĩ nhiên, tin tặc vẫn có thể tấn công vào các hệ thống được kiểm soát chặt chẽ nhiều lớp, nhưng chúng sẽ không dễ dàng đánh cắp được dữ liệu quan trọng như trước.

Các ngân hàng cần phải ngăn chặn tin tặc ngay khi bắt đầu bị tấn công, chứ không phải giải quyết hậu quả khi hệ thống đã bị chiếm quyền. Ảnh TL minh họa

Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

PV: *Phương thức kiểm tra kiểu mới như ông nói liệu đã được thực hiện ở nơi nào trên thế giới hay chưa?*

Ông Robert Trọng Trần: Tất nhiên đã có rồi. Hồi đầu năm nay, một công ty hoạt động trong lĩnh vực năng lượng ở Hồng Kông đã đồng ý tham gia một bài kiểm tra tương tự. Nhóm thử nghiệm đã tổ chức một cuộc tấn công mạng thực sự, bắt đầu từ việc xâm nhập một máy tính ở phòng kế toán của công ty này, rồi kết thúc bằng cách nắm quyền kiểm soát hệ thống đường ống dẫn gas của họ và điều chỉnh áp suất gas trong ống. Tất cả diễn ra chỉ trong một ngày. Mức áp suất gas được thay đổi chút ít, đủ để chứng minh rằng cuộc tấn công đã thành công.

Đáng nói là phần công nghệ thông tin (IT) và công nghệ vận hành (OT) của công ty năng lượng nói trên là hoàn toàn tách biệt, nhưng họ vẫn bị nhóm thử nghiệm tấn công thành công. Sau bài kiểm tra, công ty này được thông báo rằng hệ thống phát hiện/phản ứng của họ quá yếu, và những công nghệ mang tính ngăn chặn như tường lửa, phần mềm diệt virus hay IDS/IPS đang triển khai cũng không phát hiện được mã độc zero day bugs. Đây cũng là thực trạng chung mà nhiều tổ chức ở Việt Nam đang gặp phải.

Nếu công ty nào vẫn tin hệ thống sẽ không thể bị tin tặc xâm nhập, hãy thử tham gia bài kiểm tra này.

Còn tôi thì sẽ khuyên các tổ chức tài chính, ngân hàng thương mại nên nhìn nhận thật sự nghiêm túc mối nguy từ tin tặc, xem xét cân đối thêm ngân sách an ninh mạng nhằm tăng cường khả năng phát hiện/phản ứng và thiết lập thêm các biện pháp kiểm soát nhiều lớp bên trong hệ thống.

Các cơ quan thiết yếu trong lĩnh vực năng lượng, nước sạch hay viễn thông cũng cần chú ý đến vấn đề này, bởi họ sẽ là những nạn nhân đầu tiên khi chiến tranh mạng xảy ra.

Cuối cùng nhưng không kém phần quan trọng, tất cả những doanh nghiệp nào tin rằng an ninh thông tin là tối quan trọng đối với công việc kinh doanh chắn chắn sẽ phải đầu tư để bảo vệ tài sản quý giá của họ trước hiểm họa.

PV: *Quay trở lại với câu chuyện tài khoản của khách hàng Việt Nam bị "bốc hơi" như trên đã đề cập. Xin hỏi ông, vậy để phòng chống hiệu quả đối với loại tội phạm mạng, ông có thể đưa ra giải pháp và khuyến nghị gì đối với các ngân hàng Việt Nam?*

Tiêu đề: Chuyên gia nói gì về hiện tượng tiền trong tài khoản ngân hàng bị 'bốc hơi'?
Tác giả: Mai An
Nguồn: Thời báo Tài chính Việt Nam đăng ngày 28/11/2016
Đường dẫn bài viết: http://thoibaotaichinhvietnam.vn/pages/tien-te-bao-hiem/2016-11-28/chuyen-gia-noi-gi-ve-hien-tuong-tien-trong-tai-khoan-ngan-hang-bi-boc-hoi-38422.aspx

Ông Robert Trọng Trần: Có 3 biện pháp các ngân hàng nên lên kế hoạch thực hiện càng sớm càng tốt. Đầu tiên là yếu tố con người, bởi đây là điểm yếu nhất trong an toàn thông tin tại Việt Nam hiện nay. Các ngân hàng cần phải tổ chức các khóa học, tuyên truyền và rèn luyện nhân viên của mình cách nhận biết, phòng ngừa các mối nguy trực tuyến.

Ngoài ra, các ngân hàng cần thực hiện những khóa học dành cho khách hàng của mình. Tôi tin rằng ngân hàng nào thực hiện bài bản vấn đề này sẽ tạo nên điểm khác biệt và thu hút được niềm tin từ khách hàng.

Kế đến, các ngân hàng cần mời một bên thứ ba độc lập kiểm tra mức độ an toàn bảo mật và giúp xây dựng chiến lược an ninh mạng chi tiết, cụ thể. Qua cuộc kiểm tra độc lập này, lãnh đạo ngân hàng sẽ hiểu rõ được những rủi ro, điểm yếu của hệ thống. Từ đó sẽ có những đầu tư về bảo mật hiểu quả và phù hợp, chứ không phải đầu tư dàn trải như hiện nay.

Cuối cùng, trong tương lai, mỗi ngân hàng nên thành lập sẵn nhóm phản ứng nhanh cho sự cố bảo mật, có thể lập tức xử lý các trường hợp tin tặc đang cố thâm nhập vào hệ thống. Các ngân hàng cần phải ngăn chặn tin tặc ngay khi bắt đầu bị tấn công, chứ không phải giải quyết hậu quả khi hệ thống đã bị chiếm quyền.

PV: *Trân trọng cám ơn ông!*

M.A (thực hiện)