Tiêu đề: Quản trị khủng hoảng an ninh mạng: Bài học từ vụ mã độc Petya
Tác giả: Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng và Bảo mật, PwC Việt Nam
Nguồn: Đầu tư Chứng khoán, xuất bản ngày 03/07/2017
Đường dẫn bài viết: http://tinnhanhchungkhoan.vn/dau-tu/quan-tri-khung-hoang-an-ninh-mang-bai-hoc-tu-vu-ma-doc-petya-192997.html

Quản trị khủng hoảng an ninh mạng: **Bài học từ vụ mã độc Petya**

Mã độc tống tiền Petya bùng phát từ ngày 27/6/2017 đã nhanh chóng gây ảnh hưởng đến hàng loạt tổ chức, doanh nghiệp thuộc nhiều lĩnh vực hoạt động khác nhau. Nhiều nạn nhân được ghi nhận tại Ukraina, Tây Ban Nha, Hà Lan và Anh. Quy mô và tốc độ phát tán của mã độc này gợi nhắc đến cuộc tấn công an ninh mạng toàn cầu WannaCry xảy ra vào tháng 5/2017.

ĐỂ TRÁNH BỊ MÃ ĐỘC TẤN CÔNG, DOANH NGHIỆP CÓ THỂ ỨNG PHÓ NHANH BẰNG CÁCH:

- Vô hiệu hóa dịch vụ chia sẻ tập tin qua mạng trên giao thức SMBv1
- Vô hiệu hóa khả năng thực thi các macro chưa được kiểm tra trong những tập tin office, thiết lập GPO để cho phép chạy những macro nhất định và cần thiết cho doanh nghiệp;
- Sử dụng xác thực hai yếu tố cho những kết nối quan trọng từ bên ngoài vào hệ thống, ví dụ VPN và RDP
- Đảm bảo hệ thống anti-virus được cập nhật phiên bản mới nhất
- Xác định và ngăn chặn tất cả các kết nối từ những hệ thống chưa được cập nhật bản vá MS17-010 vào hệ thống chính của doanh nghiệp. Những phân đoạn mạng không dành cho vận hành hệ thống nên được ngăn cách hoàn toàn khỏi hệ thống chính.
- Ngay lập tức cách ly hệ thống bị nhiễm mã độc ra khỏi mạng doanh nghiệp để tránh phát tán mã độc ra các hệ thống khác

ROBERT TRỌNG TRẦN
Giám đốc Dịch vụ an ninh mạng và bảo mật PwC

An toàn thông tin mạng đã trở thành một trong những rủi ro đáng ngại nhất đối với các doanh nghiệp dù quy mô lớn hay nhỏ, ở mọi lĩnh vực, ngành nghề. Chúng ta phải sẵn sàng đối mặt và "sống chung" với rủi ro của các cuộc tấn công này. Doanh nghiệp cần nhận thức rõ rằng rủi ro an ninh mạng không chỉ đơn thuần là rủi ro về công nghệ thông tin, mà quan trọng hơn, đó là rủi ro kinh doanh của bất kỳ doanh nghiệp nào. Con người được xem là điểm yếu nhất trong việc bảo vệ an toàn thông tin. Vì vậy, chương trình giáo dục và nhận thức nên là vấn đề ưu tiên chiến lược hàng đầu của doanh nghiệp.

Theo đánh giá của PwC, dựa trên phân tích các trường hợp bị tấn công của doanh nghiệp, những doanh nghiệp có trang bị Bộ Quản lý khủng hoảng an ninh mạng (Cyber Crisis Management), thực hiện diễn tập và kiểm tra những kịch bản về sự cố tấn công an ninh mạng sẽ giảm thiểu được tổn thất so với những doanh nghiệp chưa có sự chuẩn bị trước. Một cuộc tấn công mạng thành công không những gây ra tổn thất nặng nề về mặt tài chính, mà còn ảnh hưởng nghiêm trọng đến uy tín của doanh nghiệp. Hơn nữa, doanh nghiệp còn phải chịu các chế tài theo quy định của pháp luật trong vấn đề bảo vệ an toàn thông tin.

Trở lại với câu chuyện mã độc Petya, nó đã tấn công hàng loạt các tổ chức ở châu Âu và Mỹ, trong đó có thể kể đến như Công ty Quảng cáo WPP, Tập đoàn Vật liệu xây dựng Saint – Gobain của Pháp; Công ty Thép Evraz và Tập đoàn Dầu khí Rosneft của Nga; Tập đoàn Thực phẩm Mondelez, Công ty Luật DLA Piper, Công ty Vận tải AP Moller – Maersk của Đan Mạch, hệ thống bệnh viện và trang thiết bị chăm sóc sức khỏe Heritage Valley Health.

Mã độc Petya lây lan bằng cách sử dụng các lỗ hổng trong hệ điều hành Microsoft Windows. Nó lan truyền nhanh chóng trong hệ thống ngay sau khi một máy tính bị nhiễm bằng cách sử dụng lỗ hổng EternalBlue trong Microsoft Windows hoặc thông qua hai công cụ quản trị Windows (đảm bảo việc lây nhiễm sẽ vẫn diễn ra cho dù hệ thống đã được cập nhật bản vá an ninh). Sau khi thâm nhập, mã độc cố gắng chiếm quyền admin, kiểm soát các công cụ quản lý hệ thống như Windows PsExec và Windows Management Instrumentation, sau đó lây nhiễm vào các hệ thống máy tính của nhiều tổ chức, mã hóa ổ cứng và đóng băng toàn bộ hệ thống của họ.

Mã độc Petya khác biệt ở phương thức tấn công trên nhiều cấp độ khác nhau. Khi được thực thi với quyền admin, nó có khả năng can thiệp vào cả bản ghi quản lý khởi động máy. Đối với quyền người dùng bình thường, Petya mã hóa các tập tin cụ thể trên hệ thống. Mã độc này cũng dùng một số phương pháp khác để đảm bảo lây lan sang nhiều thiết bị nhất có thể. Một điều đáng lưu ý, Petya không phải là mã độc tống tiền. Mục tiêu của tội phạm phát tán mã này là phá hủy tất cả các tập tin bị lây nhiễm. Vì thế, cho dù nạn nhân có trả tiền cũng không thể nào giải mã các tập tin được. Do vậy, khuyến cáo của PwC là các nạn nhân của Petya không trả tiền cho nhóm tội phạm này.

Từ những câu chuyện thực tế gần đây có thể thấy, các mã độc hiện đang trở thành một mối đe dọa ngày càng phổ biến. Số lượng các biến thể được thiết kế có chủ đích nhắm vào hệ thống mạng doanh nghiệp ngày càng tăng nhanh. Bất chấp sự bùng nổ mạnh mẽ của các loại mã độc mã hóa, các doanh nghiệp hoàn toàn có thể thiết lập chiến lược để giảm thiểu khả năng bị tấn công, hạn chế mức độ thiệt hại cũng như các đảm bảo việc phục hồi hệ thống diễn ra nhanh chóng và hiệu quả. Các chiến lược này được kết hợp

Tiêu đề: Quản trị khủng hoảng an ninh mạng: Bài học từ vụ mã độc Petya
Tác giả: Robert Trọng Trần, Giám đốc Dịch vụ An ninh mạng và Bảo mật, PwC Việt Nam
Nguồn: Đầu tư Chứng khoán, xuất bản ngày 03/07/2017
Đường dẫn bài viết: http://tinnhanhchungkhoan.vn/dau-tu/quan-tri-khung-hoang-an-ninh-mang-bai-hoc-tu-vu-ma-doc-petya-192997.html

từ nhiều khía cạnh của công tác vận hành và đảm bảo an toàn thông tin cho hệ thống, chủ yếu liên quan tới các yếu tố dưới đây.

Thứ nhất, lập kế hoạch và diễn tập đảm bảo hệ thống vận hành liên tục: Đảm bảo các hệ thống người dùng cá nhân và máy chủ trọng yếu có thể được khôi phục nhanh chóng từ những bản sao lưu và tần suất sao lưu được sắp xếp theo khung thời gian của dữ liệu mà tổ chức đã chuẩn bị trước trong trường hợp hệ thống bị mã hóa dữ liệu

Thứ hai, lập kế hoạch và diễn tập ứng phó sự cố: Đảm bảo có những quy trình chuẩn, theo đó nhân viên cùng những người chịu trách nhiệm quản lý những sự cố với mức độ ưu tiên cao trong tổ chức có thể xử lý các vấn đề liên quan đến mã độc mã hóa và khôi phục các dịch vụ cần thiết cho nhân viên cũng như khách hàng.

Thứ ba, chính sách bảo mật chặt chẽ và nâng cao nhận thức người dùng: Ngăn chặn mã độc mã hóa xâm nhập vào hệ thống công nghệ thông tin thông qua kênh phổ biến nhất là email lừa đảo bằng cách áp dụng kiểm soát chặt chẽ đối với cổng kết nối email và các phân vùng mạnh, tăng cường các hoạt động nâng cao nhận thức về an toàn thông tin của nhân viên.

Thứ tư, quản lý các bản vá lỗi và những rủi ro tồn tại trong hệ thống: Những lỗ hổng bị khai thác trong cuộc tấn công này đã được khắc phục bằng các bản vá mà Microsoft công bố vào tháng 3 và trong tuần này. Một quy trình quản lý lỗ hổng hiệu quả sẽ giúp giảm thiểu các dạng tấn công tương tự.

Doanh nghiệp cần đảm bảo hệ thống phòng chống virus, mã độc mã hóa của doanh nghiệp được cập nhật đầy đủ. Bất cứ hệ thống nào bị nhiễm mã độc mã hóa cần được cách ly hoàn toàn khỏi môi trường vận hành doanh nghiệp để tránh lây lan.

PwC không khuyến khích việc trả tiền chuộc khi bị mã độc mã hóa tấn công, trừ phi đó là mối đe dọa tới tính mạng. Việc trả tiền chuộc chỉ giúp thúc đẩy việc tấn công bằng mã độc mã hóa và cung cấp thêm các nguồn lực để tin tặc phát triển các kỹ thuật và chiến dịch mới.

Các nhà quản lý cũng nên đảm bảo rằng đội ngũ công nghệ thông tin được hỗ trợ tốt nhất để có thể nhanh chóng cập nhật các bản vá an ninh mạng cho máy người dùng và máy chủ mà Microsoft đã công bố. Các nhà quản lý nên hiểu rằng việc cập nhật các bản vá lỗi có thể tạm thời làm gián đoạn các dịch vụ công nghệ thông tin trong hệ thống, bởi vì họ cần thiết lập thêm các cơ chế kiểm soát và vô hiệu hóa các dịch vụ có nguy cơ bị tấn công.

Hãy đảm bảo rằng đội ngũ công nghệ thông tin đã lên kế hoạch hoặc đã tiến hành vô hiệu hóa các kết nối tới dịch vụ DMB từ bên ngoài vào hệ thống và ngược lại.

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