NHẬN BIẾT VÀ NGĂN CHẶN HÀNH VI ĐÁNH CẮP DỮ LIỆU

NGUYỄN CÔNG MINH
Trung tâm viễn thông 4 - Viễn thông Hà Nội

Trong lĩnh vực bảo vệ an ninh mạng nói chung và bảo mật thông tin tài khoản cá nhân trong hoạt động ngân hàng nói riêng, dữ liệu luôn là một trong những khía cạnh cốt lõi của quá trình bảo mật. Dữ liệu song hành với sự phát triển chung trong lĩnh vực bảo mật cũng như sự biến đổi của tình hình an ninh mạng toàn cầu. Bài viết tìm hiểu khái niệm trong bảo mật dữ liệu đó là Data exfiltration (đánh cắp dữ liệu), đồng thời, đưa ra cách thức phòng ngừa và ứng phó với hành vi đánh cắp dữ liệu nguy hiểm này.

1. Nhận diện hành vi đánh cắp dữ liệu

Các dữ liệu sau khi bị đánh cắp có thể đưa ra ngoài bằng các cách truyền thống trên các giao thức cho phép thông thường của hệ thống Firewall như FTP hay HTTP, chúng có thể mã hóa trước khi hành động hoặc chuyển dữ liệu này tới một máy tính hay thiết bị khác. Một số hành vi đánh cắp dữ liệu cơ bản như Data exfiltration hay cách gọi khác là Data theft, Data exportation (xuất dữ liệu trái phép) đều được hiểu là hành vi đánh cắp dữ liệu. Các hành vi đánh cắp dữ liệu này có thể được thực hiện từ các cá nhân nắm trong tay quyền truy cập vào một hệ thống máy tính, thiết bị phần cứng lưu trữ dữ liệu hoặc được thực hiện qua các chương trình, phần mềm độc hại lan truyền thông qua môi trường mạng.

Hiểu một cách khác, Data exfiltration là hình thức vi phạm bảo mật nghiêm trọng, trong đó dữ liệu có thể bị truyền hoặc sao chép mà không được sự đồng ý từ phía chủ sở hữu. Về lý thuyết, hành vi này có thể được thực hiện thông qua một loạt các kỹ thuật từ đơn giản đến phức tạp, nhưng nhìn chung, nó thường được thực hiện bởi tin tặc (tội phạm mạng) thông qua môi trường Internet. Các cuộc tấn công Data exfiltration thường được lên kế hoạch và nhắm mục tiêu cụ thể, từ đó giúp tin tặc có thể định vị và đánh cắp loại dữ liệu mà chúng muốn với xác suất thành công cao hơn.

Trên thực tế, Data exfiltration khó bị phát hiện trong nhiều tình huống, chẳng hạn như ở quá trình di chuyển dữ liệu trong hệ thống mạng nội bộ của một tổ chức, cũng như bên ngoài hệ thống mạng này. Khi những dữ liệu đó nằm trong tay tin tặc, thảm họa bảo mật hoàn toàn có thể xảy ra, đồng thời kéo theo sự sụp đổ của cả hệ thống tổ chức đó.

2. Cách thức hoạt động của Data exfiltration

Một trong những phương thức phổ biến nhất thường được tin tặc sử dụng để triển khai các chiến dịch Data exfiltration là nhằm vào mật khẩu đơn giản, dễ bị "bẻ gãy". Theo thống kê, sự tinh vi, phức tạp trong cách thức sử dụng mật khẩu sẽ tỷ lệ nghịch với xác suất trở thành mục tiêu của các chiến dịch Data exfiltration.

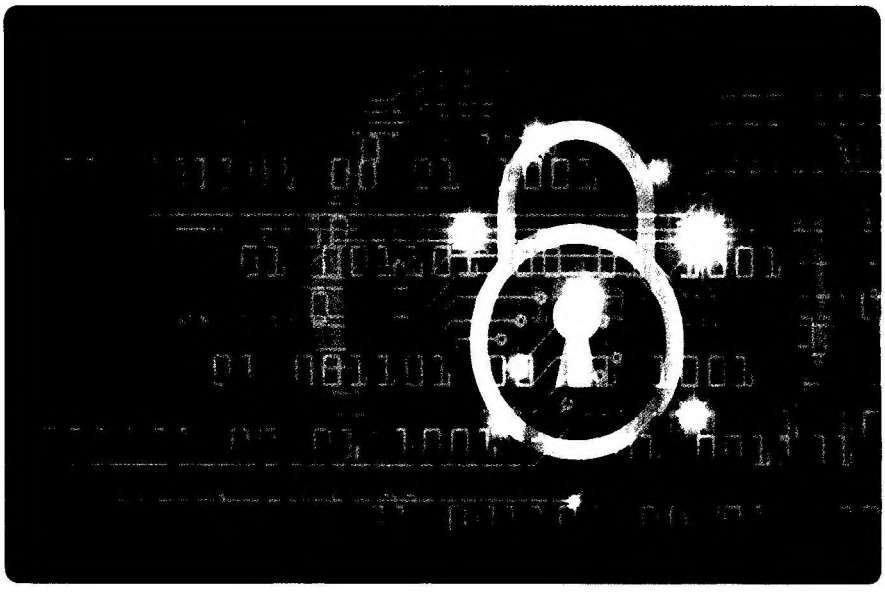
Khi mật khẩu đã bị hacker đánh cắp, tin tặc có thể truy cập vào các hệ thống mục tiêu thông qua những ứng dụng truy cập từ xa do chúng tự thiết kế hoặc mua lại của bên thứ ba, hoặc bằng cách chèn thêm một thiết bị đa phương tiện di động trong trường hợp có thêm khả năng truy cập vật lý.

Một hình thức Data exfiltration khác gọi là Advanced Persistent Threat (APT), kiểu tấn công này thường được sử dụng trong những trường hợp đã xác định rõ mục tiêu cụ thể và dữ liệu đánh cắp là những thông tin mang tính nhạy cảm cao. Mục đích chính của APT là cố gắng chiếm quyền truy cập vào hệ thống mạng mục tiêu của tổ chức, đồng thời hạn chế đến mức tối đa việc bị phát hiện trong khi đang tìm kiếm lượng dữ liệu đã nhắm mục tiêu, chẳng hạn như thông tin khách hàng, tài sản trí tuệ, hoặc thông tin tài chính... Đây đều là những loại dữ liệu cực kỳ nhạy cảm của bất cứ doanh nghiệp nào.

Hình thức đánh cắp dữ liệu này phụ thuộc rất nhiều vào những kỹ thuật xã hội như lừa đảo thông qua email (email phishing) để thử và đánh lừa các tác nhân đang hoạt động trong tổ chức mục tiêu, qua đó cài đặt một chương trình, phần mềm độc hại vào máy tính của họ và lấy đó làm "bàn đạp" để truy cập vào hệ thống mạng chung của tổ chức. Sau khi đã thâm nhập thành công, tin tặc sẽ cố gắng xác định loại dữ liệu mà chúng đang nhắm đến và bước cuối cùng sẽ là tiến hành sao chép hoặc chuyển những dữ liệu đó ra bên ngoài.

3. Phòng ngừa và ngăn chặn Data exfiltration

Các chiến dịch Data exfiltration đều được triển khai chủ yếu dựa vào các yếu tố kỹ thuật để cài đặt phần mềm độc hại vào máy tính cá nhân đang hoạt động trong hệ thống. Do vậy, biện pháp phòng ngừa hiệu quả và cấp thiết nhất đối với các tổ chức, doanh nghiệp là tăng cường đào tạo nhân viên của mình trong việc phát hiện các mối đe dọa tiềm ẩn hoạt động thông qua email,



cũng như khuyến khích nhân viên trang bị thêm kiến thức mới nhất trong lĩnh vực bảo mật, từ đó giúp họ có thể nhận diện chính xác những hành vi lừa đảo và kịp thời báo cáo vấn đề trước khi xảy ra sự cố nghiêm trọng.

Cùng với yếu tố con người, các tổ chức, doanh nghiệp cũng cần phải thiết lập những hàng rào bảo mật từ xa, được thiết kế để chủ động phát hiện sớm các mối đe dọa và chương trình độc hại tiềm năng, qua đó giúp đội ngũ bảo mật hệ thống có thể đưa ra phản ứng kịp thời và chính xác với mỗi tình huống cụ thể, hạn chế tối đa vấn đề rò rỉ, thất thoát dữ liệu.

4. Giải pháp bảo vệ điểm cuối

Bảo vệ điểm cuối (Endpoint protection) thường được sử dụng cùng với bảo mật điểm cuối (Endpoint security). Endpoint protection thường được sử dụng để mô tả các giải pháp an ninh mạng giúp giải quyết các vấn đề bảo vệ điểm cuối, bảo mật và bảo vệ Endpoint chống lại việc khai thác, tấn công và rò rỉ dữ liệu vô tình do lỗi của con người.

Một trong những nhân tố quan trọng nhất trong việc ngăn chặn Data exfiltration là bảo đảm an toàn tuyệt đối cho các thiết bị điểm cuối (Endpoint devices). Các thiết bị điểm cuối chính là nguồn cung cấp quyền truy cập dễ dàng cho tin tặc. Nói cách khác, chúng chính là cầu nối để kẻ gian xâm nhập vào hệ thống dễ dàng hơn, vì vậy, điều quan trọng là phải bảo đảm an toàn cho các thiết bị này.

Các cuộc tấn công nhắm mục tiêu và các mối đe dọa tiên tiến (APT attack) không thể được ngăn chặn nếu chỉ có các giải pháp chống virus, điều này khiến cho Endpoint protection là một giải pháp không thể thiếu trong các doanh nghiệp. Các giải pháp bảo vệ điểm cuối cung cấp các giải pháp bảo mật được quản lý tập trung nhằm bảo vệ các điểm cuối như máy chủ, máy trạm và thiết bị di động được sử dụng để kết nối với mạng doanh nghiệp.

Nền tảng bảo vệ điểm cuối toàn diện nhất tích hợp với các biện pháp bảo mật khác như lỗ hổng, bản vá và khả năng quản lý cấu hình, dẫn đến bảo vệ chủ động hơn, được coi là tiêu chuẩn vàng trên các giải pháp bảo mật phản

(Xem tiếp trang 39)

hướng tới một thứ gì đó vượt xa ứng dụng tài chính. Chúng tôi đã đi từ vị trí là ngân hàng hàng đầu cho giới trẻ, trở thành một cộng đồng người dùng theo định hướng phong cách sống. Khi làm như vậy, mối quan hệ của chúng tôi với khách hàng không bắt đầu bằng việc đăng ký tài khoản ngân hàng, như trường hợp của hầu hết các tổ chức ngân hàng, mà thay vào đó là khi người dùng quyết định tải xuống ứng dụng và đăng ký (sử dụng) nền tảng bằng địa chỉ email của họ. Khách hàng sẽ không còn đến ImaginBank chỉ để tìm kiếm các sản phẩm tài chính mà thay vào đó là sự quan tâm đến nội dung đáng giá và trải nghiệm độc đáo". Cách làm của CaixaBank, dù có thể nói là rất mạo hiểm, đã đi đúng hướng của chiến lược "Lifestyle Banking" và chỉ có những đột phá như vậy mới có thể xác định chắc chắn vị trí của ngân hàng trong lối sống của khách hàng.■

TÀI LIỆU THAM KHẢO:

1. http://www.fintechbd.com/lifestyle-banking/;

2. https://thefinancialbrand.com/98784/banking-transformed-caixabank-digital-mobile-app-platform-imagin/;

3. https://www.finextra.com/newsarticle/36055/caixabank-transforms-mobile-bank-imagin-into-lifestyle-app;

4. https://finovate.com/caixabank-launches-imaginbank-a-mobile-only-bank-for-millennials/;

5. https://www.verdict.co.uk/retail-banker-international/news/caixabank-relaunches-imagin-bank-for-young/;

6. https://www.finextra.com/blogposting/17550/part-1---top-6-mobile-banking-aspects-to-consider-when-promoting-youth-loyalty;

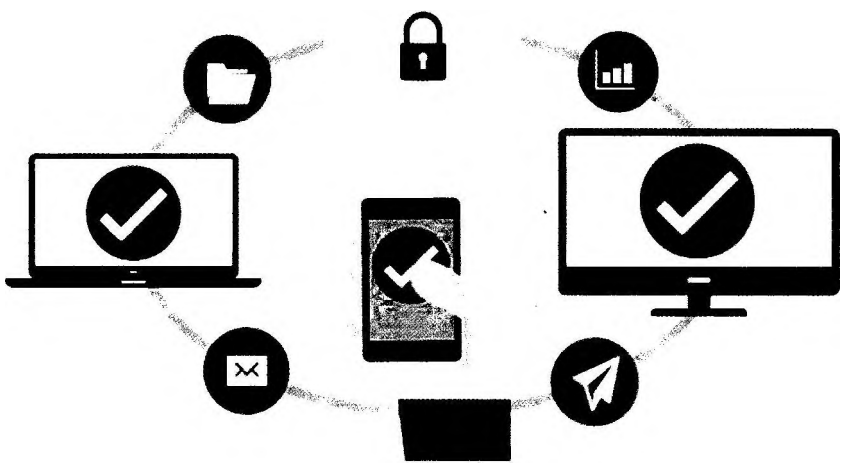
7. https://www.qulix.com/about/blog/top-6-aspects-in-building-mobile-banking-solutions-for-the-youth-part-2/;

8. https://www.zdnet.com/article/singapore-bank-dispenses-telehealth-app-with-access-to-100-medical-professionals/.

NHẬN BIẾT VÀ NGĂN CHẶN...

(Tiếp theo trang 33)

ứng trước đây. Nền tảng bảo vệ điểm cuối không chỉ đơn thuần là ngăn chặn các cuộc tấn công phần mềm độc hại, với các khả năng bảo vệ dữ liệu như mã hóa ổ đĩa, các file dữ liệu, ngăn ngừa mất dữ liệu và thậm chí kiểm soát thiết bị để bảo vệ điểm cuối toàn diện nhất có thể. Nếu không có bảo vệ điểm cuối đầy đủ, doanh nghiệp sẽ mất quyền kiểm soát dữ liệu ngay khi được sao chép vào thiết bị bên ngoài hoặc truy cập mạng tại thời điểm được thông qua điểm cuối không bảo mật. Bảo vệ điểm cuối là một thành phần quan trọng của bảo mật doanh nghiệp hiện đại, bổ sung các giải pháp bảo mật khác để bảo vệ cho dữ liệu của doanh nghiệp có thể dễ dàng thoát khỏi sự kiểm soát của tội phạm tấn công mạng.



Bảo đảm an toàn cho các thiết bị điểm cuối là khâu quan trọng trong phòng chống Data exfiltration

Việc nhận biết, ngăn chặn hành vi đánh cắp dữ liệu và ứng phó với Data exfiltration không quá phức tạp, nhưng cũng không hề đơn giản. Cái khó nằm ở chỗ các kỹ thuật và công nghệ lừa đảo vẫn không ngừng phát triển, biến đổi từng ngày, tạo điều kiện cho sự xuất hiện của những chiến dịch tấn công tinh vi hơn và gây thiệt hại nặng nề. Do vậy, các tổ chức, doanh nghiệp và đặc biệt là từng cá nhân trong hệ thống phải luôn chủ động trong mọi tình huống, cần liên tục cập nhật sự biến đổi trong thế giới bảo mật để kịp thời đưa ra những thay đổi phù hợp, cùng với đó là đẩy mạnh thực hiện các chính sách bảo mật mạnh mẽ để ngăn chặn dữ liệu bị đánh cắp khỏi tổ chức, doanh nghiệp của mình.■

TÀI LIỆU THAM KHẢO:

1.https://www.checkpoint.com/solutions/endpoint-security/;

2. https://bizflycloud.vn/;

3. https://www.fortinet.com/.