

Tiêu đề: Tội phạm công nghệ cao - vấn nạn của doanh nghiệp hiện nay

Tác giả: Robert Trọng Trần

Nguồn: Báo Đầu tư đăng ngày 30/03/2016

Đường dẫn bài viết: <http://baodautu.vn/toi-pham-cong-nghe-cao---van-nan-cua-doanh-nghiep-hien-nay-d41955.html>

Tội phạm công nghệ cao - vấn nạn của doanh nghiệp hiện nay

“Tội phạm công nghệ cao là một trong những ngành công nghiệp lợi nhuận hàng đầu trên thế giới, lớn hơn rất nhiều so với buôn lậu thuốc phiện, với lợi ích đầu tư có thể lên đến 1.425%”

30/03/2016 11:30

f Thích

1

G+1

0

Tweet



Robert Trọng Trần

Kết quả khảo sát của PwC về Thực trạng An toàn Thông tin Toàn cầu năm 2016 cho thấy, hiện tại, 45% doanh nghiệp đã có sự chỉ đạo trực tiếp của Hội đồng quản trị trong chiến lược an ninh không gian mạng (cybersecurity). Tuy nhiên Hội đồng quản trị của gần nửa số doanh nghiệp được khảo sát vẫn coi an ninh không gian mạng chỉ đơn thuần là vấn đề công nghệ thông tin mà không phải là một rủi ro bao trùm doanh nghiệp. Các doanh nghiệp cũng đang quan tâm đến các mối đe dọa công nghệ cao nhưng họ lại không theo đuổi một cách tích cực nhằm ngăn chặn và giải quyết triệt để những mối đe dọa này.

Tiêu đề: Tội phạm công nghệ cao - vấn nạn của doanh nghiệp hiện nay

Tác giả: Robert Trọng Trần

Nguồn: Báo Đầu tư đăng ngày 30/03/2016

Đường dẫn bài viết: <http://baodautu.vn/toi-pham-cong-nghe-cao---van-nan-cua-doanh-nghiep-hien-nay-d41955.html>

Cuộc khảo sát này của PwC cũng chỉ ra, riêng trong năm 2015, đã có tới 59 triệu vụ việc liên quan đến tội phạm công nghệ cao đối với các doanh nghiệp xảy ra. Tuy thế, con số này mới chỉ phản ánh một phần nhỏ thực trạng an ninh mạng hiện nay. Các tổ chức đã phải chứng kiến tỉ lệ tăng trưởng của tội phạm không gian mạng lên đến hai chữ số trong suốt 5 năm qua. Lỗ hổng bảo mật phát sinh từ các thiết bị kết nối đám mây đã nhảy vọt tới 152% trong năm 2015 so với cùng kỳ năm ngoái. Cùng với sự tăng trưởng của mạng lưới vạn vật kết nối Internet (Internet of Things), có thể dự đoán số lượng lỗ hổng bảo mật còn tăng lên nhanh chóng, đồng thời thiệt hại gây ra bởi tội phạm không gian mạng có thể trầm trọng hơn: với 7% số vụ có giá trị thiệt hại lớn hơn 1 triệu USD.

Tại Việt Nam, rất nhiều nhà lãnh đạo các doanh nghiệp vẫn nghĩ rằng các cuộc tấn công công nghệ cao chỉ xảy ra đâu đó đối với các doanh nghiệp khác. Nhiều doanh nghiệp “mất bò mới lo làm chuồng” - chỉ lo bảo mật thông tin khi có tấn công thực sự xảy ra với doanh nghiệp mình.

Một ví dụ cụ thể về hậu quả của quan điểm nêu trên đó là hiện nay số lượng các tổ chức Việt Nam và nước ngoài trở thành nạn nhân của phần mềm tống tiền (ransomware) ngày càng gia tăng. Nạn nhân mới nhất là một bệnh viện ở Los Angeles đã phải chấp nhận chi trả 17.000 USD cho bọn tội phạm công nghệ cao để mở khóa hệ thống công nghệ của bệnh viện bị kẻ tấn công mã hóa. Một công ty đa quốc gia Việt Nam cũng đã bị tấn công bởi một phần mềm độc hại gây ngừng trệ hoạt động toàn bộ hệ thống của họ trong suốt 2 ngày.

Thật không may đây mới chỉ là một vài ví dụ trong danh sách rất dài những doanh nghiệp đã trở nên bất lực trước những trò lừa đảo và phải móc hầu bao chi trả cho tội phạm công nghệ cao để có thể tiếp tục công việc kinh doanh của mình.

Vậy cơ chế hoạt động của phần mềm tống tiền như thế nào và nguy hại ra sao đến hoạt động kinh doanh và danh tiếng của doanh nghiệp?

Những nhóm tội phạm có tổ chức đã lợi dụng điểm yếu của doanh nghiệp nhằm thâm nhập vào mạng nội bộ, từ đó chúng sẽ ngăn chặn công ty truy cập vào chính hệ thống của mình bằng cách mã hóa dữ liệu trên ổ cứng hoặc cơ sở dữ liệu của máy chủ. Điều này hiển nhiên sẽ làm gián đoạn hoạt động kinh doanh của doanh nghiệp.

Hậu quả là doanh nghiệp sẽ bị ép buộc nộp tiền chuộc thông qua phương thức thanh toán trực tuyến cụ thể nào đó để có thể truy cập trở lại vào hệ thống của chính mình.

Tiêu đề: Tội phạm công nghệ cao - vấn nạn của doanh nghiệp hiện nay

Tác giả: Robert Trọng Trần

Nguồn: Báo Đầu tư đăng ngày 30/03/2016

Đường dẫn bài viết: <http://baodautu.vn/toi-pham-cong-nghe-cao---van-nan-cua-doanh-nghiep-hien-nay-d41955.html>

Đây là một trong số vô vàn ví dụ của tội phạm công nghệ cao. Câu hỏi đặt ra là tại sao loại hình tội phạm này lại phát triển nhanh đến vậy? Đơn giản bởi tội phạm công nghệ cao thu được lợi nhuận lớn hơn rất nhiều so với buôn lậu thuốc phiện. Đây chính là một trong những ngành công nghiệp lợi nhuận hàng đầu trên thế giới. Bản báo cáo gần đây của công ty Trustwave cho thấy nhóm tội phạm công nghệ cao thu được lợi ích **đầu tư** lên đến 1.425% trong việc mua những bộ công cụ khai thác điểm yếu và phần mềm tống tiền, khiến cho các tổ chức phải trả tiền cho những kẻ tấn công đã cài những phần mềm độc hại lên máy tính của họ.

Loại hình tội phạm này đang bùng nổ cũng là nhờ Phần mềm độc hại được cung cấp như dịch vụ (MaaS), đây là một mô hình kinh doanh rất được ưa chuộng trên thị trường chợ đen trực tuyến. Khi sử dụng hình thức MaaS, bất kỳ tội phạm trên mạng nào cũng có thể thực hiện các cuộc tấn công gây gián đoạn hoạt động của các tổ chức ở bất kỳ đâu trên toàn thế giới. Và thậm chí chúng cũng không cần bất cứ công cụ hay kỹ năng cần thiết nào để thực hiện tấn công. Chúng có thể đơn giản là trả tiền cho một kẻ nào đó hoặc thuê những công cụ cần thiết để thực hiện.

Vậy liệu doanh nghiệp còn có khả năng tiếp tục bị tấn công khi số tiền chuộc đã được trả hay không? Câu trả lời là có – vì kẻ tấn công giờ đã nắm rõ điểm yếu của hệ thống, và chúng cũng biết doanh nghiệp sẵn sàng chi trả tiền chuộc. Điều này giải thích tại sao lãnh đạo các doanh nghiệp nên có nhận thức đúng về an ninh không gian mạng, không kém hơn so với hiểu biết về các lĩnh vực khác của doanh nghiệp. Tội phạm công nghệ cao có thể xảy đến với bất kỳ doanh nghiệp nào và hủy hoại danh tiếng của họ.

Vì thế, việc cấp bách cần thực hiện đối với doanh nghiệp là đánh giá tình trạng an ninh không gian mạng hiện tại, để biết liệu doanh nghiệp đã bảo vệ tốt dữ liệu khách hàng và danh tiếng của mình hay chưa, hay là đang mở sẵn cửa để các thông tin, dữ liệu của công ty rò rỉ và xuất hiện trên trang nhất các báo.

Các doanh nghiệp nên tìm đến các công ty cung cấp dịch vụ an ninh không gian mạng với phạm vi mang tính toàn diện nhằm hỗ trợ các hoạt động đánh giá, xây dựng và quản lý năng lực của doanh nghiệp và ứng phó khi có sự cố hay khủng hoảng xảy ra. Các dịch vụ này được thiết kế để mang đến cho doanh nghiệp sự tự tin, thấu hiểu các mối đe dọa và điểm yếu của chính mình và đảm bảo an ninh cho môi trường hoạt động của doanh nghiệp.

Robert Trọng Trần (Trưởng phòng Cao cấp, Dịch vụ An ninh mạng, Công ty PwC Việt Nam)