

Bùng nổ thương mại điện tử: Hiểm họa từ thế giới ảo

21:43 04/04/2018

Sự phát triển công nghệ kéo theo sự bùng nổ của thương mại điện tử (TMĐT), dẫn đến các rủi ro an ninh mạng như tấn công mạng và tội phạm mạng, xâm phạm quyền riêng tư, khai thác trái phép dữ liệu cá nhân cho mục đích thương mại và phi thương mại... đang ngày càng gia tăng trên Internet.

Rò rỉ thông tin người dùng

Năm 2016, ngành TMĐT Việt Nam đạt tổng doanh thu 5 tỷ USD. Đến năm 2017, đã có 21 DN khởi nghiệp trong lĩnh vực bán lẻ trực tuyến này với tổng vốn đầu tư nước ngoài lên đến 84 triệu USD. Việt Nam đang là môi trường hấp dẫn đối với bán lẻ trực tuyến. Điều này thể hiện qua số lượng các vụ sáp nhập và mua lại các hãng bán lẻ tại Việt Nam (hơn 500 vụ, giá trị mua lại là 5,8 tỷ USD).

Điển hình, năm 2015, Công ty Transcosmos Nhật Bản mua lại website Hotdeal.vn. Thailand Central Group liên tục thôn tính các DN Việt như Nguyễn Kim, Big C và Zalora. Năm 2016, Lazada đã bị mua lại bởi Alibaba với tổng giá trị 1 tỷ USD. Năm 2017, JD.com của Trung Quốc đầu tư vào Tiki.vn, công ty đầu tư SEA của Singapore thôn tính DN TMĐT khởi nghiệp Việt như Foody, Shopee, Giao hàng tiết kiệm...

Sự tăng trưởng mạnh mẽ của TMĐT, đi kèm với đó là gia tăng các rủi ro về an ninh mạng.

Ngoài các rủi ro đã được nhận diện - như tấn công mạng và tội phạm mạng; các rủi ro khác, gồm: Xâm phạm quyền riêng tư và khai thác trái phép dữ liệu cá nhân cho mục đích thương mại cũng như phi thương mại; vấn đề tin giả, thông tin không chính xác; phát ngôn thù ghét cũng đã gia tăng đáng kể với người dùng Internet, với DN.

Năm 2017, xảy ra vụ việc, nhân viên hãng Hàng không Vietnam Airlines đã để lộ thông tin khách hàng cho các hãng taxi. Theo đó, chị T.H (Hà Nội), khiếu nại về vụ việc này sau khi nhận được tin nhắn của một hãng taxi chào mời đi từ Nội

Bài về trung tâm Hà Nội, chỉ vài phút sau khi chuyến bay của chi hạ cánh.



Bùng nổ thương mại điện tử và kết nối xã hội tạo ra những hiểm họa từ không gian mạng

Có thể thấy, chính sách an ninh mạng ở Việt Nam đang ở giai đoạn bước ngoặt, đòi hỏi phải được đánh giá lại và có những bước tin mới để ứng phó với những thách thức mới để đảm bảo thúc đẩy tăng trưởng kinh tế.

Theo đánh giá của Viện Nghiên cứu chính sách và phát triển truyền thông (IPS), các rủi ro nêu trên đang là thách thức rất lớn Việt Nam phải đối mặt trong bối

cảnh mở rộng nhanh chóng không gian mạng và kết nối Internet, bùng nổ TMĐT và kết nối xã hội trên không gian mạng.

Trong khi đó, nhận thức của người dân, DN, chính quyền, truyền thông về quyền riêng tư... ở Việt Nam còn hạn chế; hiểu biết và kỹ năng của người dân, DN về sử dụng Internet an toàn còn thấp và chưa theo kịp với tốc độ phổ biến của công nghệ và các thiết bị kết nối; các thiết chế thực thi và bảo vệ quyền riêng tư gồm hệ thống pháp luật, hiệu lực của các cơ quan thực thi, cơ chế giải quyết tranh chấp, xử lý vi phạm hành chính và hình sự liên quan đến tấn công mạng của Việt Nam vẫn còn yếu và thiếu hiệu quả.

Việt Nam đang quan tâm ứng phó với hành vi tấn công mạng, tấn công các cơ sở hạ tầng thông tin quan trọng quốc gia (hạ tầng viễn thông, hệ thống tài chính và kết nối thanh toán...). Song, 3 vấn đề trọng yếu gồm “tin giả và thông tin không chính xác”, “phát ngôn thù ghét”, “khai thác thông tin cá nhân cho mục đích thương mại” trên không gian mạng đều chưa được quan tâm quản lý đúng mức.

IPS cho rằng, hoạt động và điều phối hợp tác giữa các cơ quan nhà nước có liên quan trong lĩnh vực an ninh mạng (Bộ Công an, Bộ Quốc phòng, Bộ Thông tin Truyền thông) còn chưa có một chiến lược tổng thể mang tầm quốc gia.

Các hoạt động hợp tác quốc tế nhằm ngăn ngừa tấn công mạng, tội phạm mạng xuyên quốc gia ngày càng trở nên quan trọng khi Internet là không gian toàn cầu vượt khỏi chủ quyền truyền thống, cũng như năng lực tài phán và thực thi pháp luật riêng biệt của mỗi quốc gia. Tuy nhiên, Việt Nam tham gia vào các nỗ lực quốc tế, các sáng kiến và cơ chế hợp tác toàn cầu về an ninh mạng còn hạn chế.

Từ thực trạng nêu trên, IPS khuyến nghị, Việt Nam cần có cách tiếp cận chính sách toàn diện, đa giải pháp cho vấn đề an ninh mạng với sự tham gia của cả Nhà nước, DN và người dùng. Các giải pháp pháp lý bằng luật và những quy định dưới luật, cũng như các giải pháp về kỹ thuật sẽ là không đủ để giải quyết những thách thức phức hợp và xuyên quốc gia về an ninh mạng.

Để bảo vệ quyền riêng tư và tài sản dữ liệu người dùng (cá nhân, DN), theo IPS, Việt Nam không cần thiết phải ban hành thêm các luật mới mà chỉ cần cụ thể hóa thêm các quy định pháp luật hiện hành để bảo vệ quyền riêng tư và tài sản dữ liệu người dùng (cá nhân, DN).

Đơn cử, các quy định sẵn có trong Bộ luật Dân sự 2015 (nội dung về quyền đối với đời sống riêng tư của cá nhân); trong Luật Trẻ em 2016 (nội dung về bảo vệ

trẻ em trên không gian mạng); trong Luật DN 2015 (nội dung về xử lý thông tin, dữ liệu cá nhân người dùng khi DN tiến hành mua bán, chia, tách, hợp nhất, sáp nhập). Tuy nhiên, việc cụ thể hóa các quy định về bảo vệ dữ liệu cá nhân cũng cần phải xem xét và cân bằng với việc bảo đảm quyền tiếp cận thông tin trong Luật Tiếp cận thông tin 2015, bảo đảm lợi ích công cộng.

Các cơ chế để giải quyết việc xâm phạm quyền riêng tư và tài sản dữ liệu, giải quyết tranh chấp, xung đột giữa người dùng và DN, cũng như DN với DN (quan hệ dân sự), giữa người dùng cá nhân, DN với Nhà nước (quan hệ hành chính) hiện nay ở Việt Nam, theo IPS hầu như không hiệu quả, trong dài hạn cần phải tăng cường vai trò của tòa án và các quy trình tư pháp.

IPS cho rằng, cần có chương trình truyền thông và giáo dục sâu rộng về an toàn Internet để nâng cao nhận thức lẫn kỹ năng của người dùng. Các chương trình giáo dục cần rà soát lại để cập nhật và giáo dục cho trẻ em về Internet ngay từ trong trường học.

Anh Đức