AN NINH MẠNG VÀ BẢO MẬT DỮ LIỆU VIỆT NAM: KHI CHUÔNG REO…

Xã hội

Xã hội mạng cũng có những vấn đề không khác với xã hội thực. Cũng hoàn toàn không phải ngẫu nhiên khi năm 2007 này được coi là một năm mà hoạt động an ninh mạng và bảo mật dữ liệu là mối quan tâm hàng đầu…

Chuông đã reo nhưng…

2006 là một năm được coi là phát triển mạnh mẽ của những ứng dụng mạng, giải pháp CNTT thì cũng chính là thời điểm bùng nổ những cuộc tấn công khiến giới dùng mạng tại Việt Nam thường xuyên phải giật mình thon thót. Nạn nhân không trừ một ai, từ người dùng phổ thông cho tới cả những doanh nghiệp vốn thành công nhờ Internet và thậm chí là cả những website công.

Những tội phạm mạng vốn từ lâu đã được coi như sự tồn tại khó tránh trong một xã hội mạng quá đa dạng nhưng quả thật, khi nó liên tiếp xảy ra và trở thành mối đe doạ xung quanh chúng ta thì ở một khía cạnh nào đó, những cuộc tấn công này tự nó lại chính là hồi chuông cảnh báo và khiến tất cả chúng ta phải quan tâm hơn đến hệ thống bảo vệ mình.

Thế nhưng, lo lắng bị tấn công có lẽ chưa đồng nghĩa với việc biết cách bảo vệ mình và nâng cao hệ số an toàn cho mình, cũng giống như việc biết nguy hiểm nhưng không phải ai ai cũng thấy động để đủ sự quan tâm. Để rồi khi những cuộc tấn công xảy ra thì đành ngậm ngùi vì chưa đủ biện pháp phòng tránh.

Theo ông Vũ Duy Khánh, Giám đốc Trung tâm ứng cứu khẩn cấp máy tính Việt Nam- VNCERT, mặc dù ở Việt Nam chưa có những vụ tấn công gây thiệt hại lớn nhưng cần biết đến những thống kê thiệt hại như riêng virus chẳng hạn cũng lên tới hàng trăm, triệu USD... Ngoài ra đối với những cơ sở dữ liệu nhạy cảm như cơ quan đảng nhà nước mà bị làm sai lệch dữ liệu chứ chưa phải là ăn cắp dữ liệu thì đã dẫn đến hậu quả rất là nghiêm trọng.

Việt Nam cũng đã hình thành nhiều trung tâm nghiên cứu, nhiều cơ quan cảnh báo như Trung tâm ứng cứu máy tính khẩn cấp VNCERT, Bộ Bưu chính viễn thông, nơi tiếp nhận thường xuyên những vụ tấn công, những sự cố liên quan đến máy tính.Hay quen thuộc hơn nữa là Trung tâm an ninh mạng BKIS với những phần mềm diệt virus cập nhật liên tục, với những cảnh báo sớm và cả những giải pháp an toàn được người dùng tin cậy.

Thế nhưng, dường như, có một điều khá mâu thuẫn là phần đa những trung tâm này chỉ được viện đến khi "sự đã rồi".

Cũng theo ông Vũ Duy Khánh, Giám đốc VNCERT trao đổi, mức đầu tư CNTT của các doanh nghiệp Việt Nam cho bảo đảm an toàn thông tin thường thấp hơn so với mặt bằng chung của thế giới.

Ý thức - lời giải của sự mâu thuẫn?

Xin miễn bàn tới ý thức của những người tấn công cũng như căn nguyên của những sự phá hoại. Bởi, cũng giống như trong một môi trường xã hội cạnh tranh ngoài đời thực, những cuộc đột nhập, tin tặc là điều không thể không có. Việc nâng cao ý thức của chính những nhà mạng và người dùng là điều cần thiết hơn hết.

Tháng 3 vừa qua, một hội thảo và triển lãm khá qui mô về an ninh mạng và bảo mật dữ liệu đã được tổ chức tại Hà Nội. Cuộc gặp gỡ các bên này đã thu nhận rất nhiều ý kiến chuyên gia mà tập trung lớn nhất có lẽ là ý thức của chính những người cần được bảo vệ. Đó là người dùng cá nhân, là doanh nghiệp, là các nhà cung cấp mạng… Đó là những thông tin quý giá, những thông tin luôn là lợi ích vươn lên của các doanh nghiệp trong thời buổi cạnh tranh.

Điều này đã được ông Clarence Phua, công ty Sophos đề cập: "Làm sao phải đảm bảo hoạt động cho hạ tầng mạng, rồi nâng cấp máy tính, máy chủ đã khiến các doanh nghiệp lo lắng. Tuy nhiên, thực tế hiện nay cho thấy là đầu tư cho bảo mật dữ liệu còn quan trọng hơn nhiều".

Ý thức ở đây còn là sự hợp tác, sự cùng ngồi lại với nhau để giúp đỡ nhau của các bên. Bởi trên thực tế, sự hợp tác chặt chẽ giữa các bên mới có thể tạo ra những tiếng nói chung. Ông Nguyễn Tử Quảng, Giám đốc Trung tâm An ninh mạng BKIS chia sẻ: "Khung pháp lý rồi ý thức là một chuyện nhưng cũng không thể không nhắc tới sự làm việc giữa các bên cũng là điều cần lưu ý. Khi người ta không hiểu phải làm thế nào mà anh cứ cảnh báo thì đôi khi nó cũng mất tác dụng. Hãy để cho người dùng hiểu rằng an ninh mạng cũng là những điều rất đơn giản thôi, giống như bạn phải trang bị một hệ thống an ninh cho chính ngôi nhà của bạn vậy, từ lúc thiết kế cho tới khi bạn sống ở đó. Như thế, hiện nay, thuê chuyên nghiệp chính là điều mang lại những thuận lợi trông thấy được".

Ý thức ở đây chính là sự đề phòng, là chiến lược, là tầm nhìn để bảo đảm cho sự an toàn của chính bản thân mình. Và tất nhiên, ý thức chính là nền tảng để đi cùng với rất nhiều những hệ thống phụ trợ khác đang và sẽ được hình thành như khung pháp lý, như hệ thống sản phẩm bảo mật…

Còn nhiều việc phải làm

Nhiều người vẫn nghĩ rằng những nguy cơ về an ninh mạng, những sự rò rỉ về nhưng vấn đề an ninh mạng và bảo mật cần được đảm bảo trong tất cả những sản phẩm mà bạn sử dụng ở bất kỳ

môi trường mạng hay không mạng.

Ông Chuck Trent, Phó Chủ tịch Tập đoànPhụ trách CNTT khu vực châu Á - TBD và Nhật Bản tập đoàn Cisco System cho biết: Hiện nay, nhiều người vẫn nghĩ an ninh, bảo mật là ở máy chủ, là mạng thế nhưng, hệ thống bị tấn công thì không loại trừ bất kỳ sản phẩm nào, bất kỳ bạn là ai. Rất nhiều khách hàng khi tìm đến với chúng tôi đã từng gặp phải những vấn đề nằm ngay ở chính những thiết bị cầm tay như điện thoại di động chẳng hạn. Những điều mà có lẽ ít khi họ ngờ tới. Bởi vậy, tầm nhìn, dự đoán và cảnh báo là điều mà tất cả chúng ta luôn phải lưu ý.

Rất nhiều chuyên gia mà phóng viên chúng tôi có dịp trao đổi tại Hội thảo về An ninh và bảo mật dữ liệu đầu tiên tại Việt Nam đã cho rằng, bất kỳ môi trường nào thiếu cảnh giác đều có thể trở thành khu vực bị tấn công. Rất nhiều dự đoán cũng đã được đưa ra mà điểm nóng của bảo mật thời gian tới đây theo nhiều người chính là lĩnh vực di động, là mạng không dây. Bởi lẽ, khi mạng viễn thông ngày càng phát triển, khi mạng không dây trở nên "chằng chịt" như một mạng nhện trong thành phố thì cũng tạo ra rất nhiều khó khăn về quản lý, về việc phổ biến những kiến thức cho người dùng.

TS. Đại tá nguyễn Viết Thế, Cục trưởng Cục Công nghệ Tin học nghiệp vụ - Tổng cục Kỹ thuật Bộ công an cũng cho rằng: "Khi mà các loại điện thoại thông minh, các dịch vụ nội dung ra đời chóng mặt mà người dùng đôi khi không đề phòng cũng rất dễ bị lợi dụng, bị đánh cắp thông tin mà thậm chí người dùng cũng không hề hay biết".

Rõ ràng, khi xã hội thông tin, không gian mạng ngày càng phát triển thì cũng đồng nghĩa với việc phát triển không ngừng của những hình thức tấn công, đánh cắp thông tin, những mối đe doạ về an ninh bảo mật. Bởi vậy, cũng quan trọng không kém để xây dựng một nền tàng cho an ninh mạng và bảo mật chính là ý thức luôn sẵn sàng và một tầm nhìn mang tính cảnh báo.

Minh Châm