RỦI RO VÀ PHÒNG TRÁNH RỦI RO TRONG THƯƠNG MẠI ĐIỆN TỬ

Giảng viên: **Nguyễn Phương Chi**
Email: **chinp@ftu.edu.vn**

Tháng 2/2000, một tin tặc 15 tuổi tự xưng là Mafiaboy tấn công các địa chỉ internet của Yahoo, Dell, CNN, Amazon.com và eBay. Virus của người này đã tấn công máy tính của những hãng trên bằng cách tạo ra lệnh gửi các yêu cầu giả liên tục trong suốt 6 ngày, làm tê liệt hệ thống trong 16 giờ liền. Theo ước tính mỗi ngày Amazon.com có tới hàng nghìn đơn đặt hàng lớn nhỏ với doanh thu trung bình xấp 500.000 USD/ ngày thì việc hệ thống máy tính tê liệt trong vòng 16 giờ đồng hồ sẽ làm hãng mất rất nhiều đơn đặt hàng, đó còn chưa kể những thiệt hại về mất uy tín của hãng đối với khách hàng

Các hacker khai thác các lỗ hổng của các hệ điều hành như Windows2000, Windows Server 2000 và các bộ Office nổi tiếng của hãng để tạo ra các virus có sức công phá và mức độ lây lan kinh khủng. Vì các phần mềm của hãng Microsoft được sử dụng rộng rãi nên hậu quả đối với các mạng máy tính trên toàn thế giới là rất lớn. Chẳng hạn như vào tháng **7/2001**, Virus CodeRed tấn công phần mềm mạng của Microsoft. Con bọ này phát hiện điểm yếu trong hệ thống máy tính và tự nhân bản trong quá trình truy nhập. Tổng thiệt hại trong sự cố mà nó gây ra lên đến 2.6 tỷ

Một số rủi ro trong TMĐT

- Rủi ro về dữ liệu
- Rủi ro về công nghệ
- Rủi ro về thủ tục và quy trình giao dịch
- Rủi ro về pháp lý và các tiêu chuẩn công nghiệp
- Rủi ro khác

Nhóm rủi ro về dữ liệu

- Liên quan đến việc bảo mật các dữ liệu của doanh nghiệp
- Các thông tin cá nhân của khách hàng, đối tác
- Nội dung các đơn chào hàng , hỏi hàng , đặt hàng
- Thông tin mật về những cuộc đấu thầu , đàm phán hợp đồng hay
- Danh mục sản phẩm mục mật của doanh nghiệp…

Nhóm rủi ro về công nghệ

- Sự xâm nhập và lây lan của virus
- Tấn công của tin tặc, trộm cắp trên mạng
- Sự giảm sút hiệu quả của dịch vụ thương mại điện tử khi công nghệ của doanh nghiệp chưa đáp ứng được với trình độ của dịch vụ sử dụng
  - Cơ sở vật chất
  - Trình độ của người sử dụng

Nhóm rủi ro về đường truyền & quy trình giao dịch

- *Nhóm rủi ro đường truyền*
- *Các thủ tục , quy trình giao dịch*
  - Quy trình giao dịch thiếu chặt chẽ của các doanh nghiệp
  - Sơ xuất trong việc chứng thực các thông tin về người mua và đối tác…

Nhóm rủi ro về pháp lý & các tiêu chuẩn công nghiệp

- *Rủi ro về pháp lý*
- *Rủi ro về các tiêu chuẩn công nghiệp*

Một số dạng tấn công TMĐT

- Virus
- Tin tặc (hacker) và các chương trình phá hoại (cybervandalism)
- Tấn công từ chối dịch vụ (DOS – Denial of Service Attack)
- Kẻ trộm trên mạng (Sniffer)
- Phishing – kẻ giả mạo

Virus tấn công vào thương mại điện tử thường gồm 3 loại chính: virus ảnh hưởng tới các tệp (file) chương trình (gắn liền với những file chương trình, thường là .COM hoặc .EXE), virus ảnh hưởng tới hệ thống (đĩa cứng hoặc đĩa khởi động), và virus macro. Virus macro là loại virus phổ biến nhất, chiếm từ 75% đến 80% trong tổng số các virus được phát hiện. Đây là loại virus đặc biệt chỉ nhiễm vào các tệp ứng dụng soạn thảo, chẳng hạn như các tệp ứng dụng của MS Word, Excel và Power Point . Khi người sử dụng mở các tài liệu bị nhiễm virus

Ngày 1-4-2001, tin tặc đã sử dụng chương trình phá hoại tấn công vào các máy chủ có sử dụng phần mềm Internet Information Server (IIS) của Microsoft nhằm làm giảm uy tín của phần mềm này và rất nhiều nạn nhân như hãng hoạt hình Walt Disney, Nhật báo phố Wall ...đã phải gánh chịu hậu quả cả về tài chính và uy tín.

gây trở ngại cho hoạt động của nhiều doanh nghiệp. Vụ tấn công DOS điển hình đầu tiên xảy ra vào tháng 2-2000, các hoạt động tấn công liên tục khiến hàng loạt website trên thế giới ngừng hoạt động trong nhiều giờ, trong đó có những website hàng đầu như: eBay ngừng hoạt động trong 5 giờ, Amazon gần 4 giờ, CNN gần 3.5 giờ, E-Trade gần 3 giờ, Yahoo và Buy.com và ZDNet cũng ngừng hoạt động từ 3 đến 4 giờ. Ngay cả người khổng lồ Microsoft cũng đã từng phải gánh chịu hậu quả của những cuộc tấn công này. Ở Việt Nam,cũng đã có rất nhiều doanh nghiệp bị tấn công dưới hình thức này.

Kẻ trộm trên mạng (sniffer) là một dạng của chương trình theo dõi, nghe trộm, giám sát sự di chuyển của thông tin trên mạng. Khi sử dụng vào những mục đích hợp pháp, nó có thể giúp phát hiện ra những yếu điểm của mạng, nhưng ngược lại, nếu sử dụng vào các mục đích phi pháp, các phần mềm ứng dụng này sẽ trở thành các mối hiểm hoạ lớn và rất khó có thể phát hiện. Kẻ trộm sử dụng các phần mềm này nhằm lấy cắp các thông tin có giá trị như thư điện tử, dữ liệu kinh doanh của các doanh nghiệp, các báo cáo mật...từ bất cứ nơi nào trên mạng.

đã bị kẻ giả mạo tấn công ăn cắp thông tin của khách hàng. Hay Vào 17/12/2003 một số khách hàng của eBay nhận được email với thông báo rằng hiện tại tài khoản của họ tạm ngừng hoạt động cho tới khi họ kích vào đường link được cung cấp trong email và cập nhật thông tin về thẻ tín dụng, cùng với các thông tin cá nhân khác như ngày sinh, tên thời con gái của mẹ, số Pin của thẻ ATM. Đường link trong địa chỉ email kết nối tới trang web của ebay nhưng đây không phải là trang web thật của ebay mà chỉ là một trang web giả mạo có logo và hình thức giống với trang web ebay thật. PayPal một trang web giải pháp thanh toán cũng là đối tượng thường xuyên bị giả mạo. Kẻ giả mạo Paypal đã xây đường URL cải trang giống URL của Paypal bằng cách sử dụng ký hiệu @ (http://paypal.com@218.36.41.188/fl/login.html). Thường thì các server bỏ qua các ký tự trước @ và chỉ sử dụng những ký tự sau nó. Như vậy là khách hàng chỉ có thể nhìn thấy đường link trong mail như http://paypal.com Chính vì vậy mà khách hàng đã không nhận ra được là mình đang bị tấn công từ các tin tặc và đã cung cấp nhưng thông tin cá nhân và tài khoản

Những biện pháp cơ bản đảm bảo an toàn trong giao dịch TMĐT

- Sử dụng kỹ thuật mã hóa thông tin
- Phong bì số
- Chứng thư số hóa

Những biện pháp cơ bản nhằm đảm bảo an toàn cho hệ thống TMĐT

- Tường lửa
- Mạng riêng ảo
- Sử dụng mật khẩu đủ mạnh
- Phòng chống virus
- Giải pháp an ninh nguồn nhân lực
- Giải pháp về trang thiết bị an ninh mạng