ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ

BÀI GIẢNG
TIN HỌC CƠ SỞ

BÀI 16. ĐẠO ĐỨC VÀ PHÁP LÝ ĐỐI VỚI CNTT

Giảng viên: ĐÀO KIẾN QUỐC
Mobile 098.91.93.980
Email: dkquoc@vnu.edu.vn

NỘI DUNG

- Các loại tội phạm tin học
- Pháp luật Việt Nam liên quan tới tội phạm CNTT

MỘT SỐ HOẠT ĐỘNG CÓ MỤC ĐÍCH XẤU

- Tấn công trực tiếp hoặc xâm phạm các hệ thống thông tin như tạo ra và phát tán vi-rút, vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính gây rối loạn hoạt động, phong toả hoặc lấy cắp thông tin, làm biến dạng, làm huỷ hoại các dữ liệu của máy tính
- Vi phạm bản quyền phần mềm và nội dung thông tin
- Lạm dụng mạng máy tính để phạm tội như lừa đảo tài chính qua mạng; phát tán các tài liệu phản văn hoá, vi phạm an ninh quốc gia; sử dụng Internet để nhằm mục đích đe doạ, quấy rối, xúc phạm đế danh dự , nhân phẩm của người khác
- Vi phạm tính riêng tư qua thư rác (Spamming) và phần mềm quảng cáo (Adware)

VIRUS VÀ SÂU (WORM)

- Virus là các đoạn mã chương trình có mục đích gây nhiễu, thậm chí phá hoại có các đặc tính sau:
  - Chương trình tương đối nhỏ, hiệu quả cao và thường có các cơ chế chống phát hiện.
  - Virus có khả năng lây lan, khi lọt vào một máy nó chiếm quyền điều khiển của hệ điều hành để tự nhân bản nhằm lây lan từ máy này sang máy khác
  - Phân biệt virus: phải có vật chủ là một file hay đoạn mã điều khiển của vùng boot của đĩa. Chính vì tính năng tương tự với virus sinh học này mà người ta gọi các chương trình có khả năng tự nhân bản phải nhờ vật chủ này là virus.
- Sâu là chương trình độc lập, không cần vật chủ. Sâu thực hiện lây lan thường theo đường mạng. Sâu không nhiễm vào file
- Tuy nhiên khi nói về virus nói chung người ta vẫn hàm ý nói cả virus và worm.

CƠ CHẾ CỦA VIRUS FILE

- Ký sinh vào một file chương trình. Khi thi hành, chương trình này, đoạn mã virus sẽ chiếm một vùng bộ nhớ để sao mã của virus và sửa một số dịch vụ (một số ngắt, chủ yếu liên quan đến việc ghi fiel) của hệ điều hành. Khi đó máy tính đã bị nhiễm virus
- Sau khi đã máy đã nhiễm, nếu chạy một chương trình khác, các dịch vụ đã bị sửa đổi sẽ làm việc gắn đoạn mã của virus đã có trong bộ nhớ vào file chương trình chạy và ghi lại vào đĩa. Khi đó virus đã thực hiện được việc lây nhiễm.

VIRUS BOOT

- Boot là vùng đĩa ghi chương trình khởi động của hệ điều hành. Khi khởi động máy, nhân khởi động của hệ điều hành trong ROM sẽ chạy trước, rồi tìm vùng boot để thi hành.Đến lượt mình boot sẽ tải các thành phần của hệ điều hành từ đĩa vào bộ nhớ.
- Virus boot gắn mã của mình vào vùng boot. Khi khởi động máy bằng một đĩa nhiễm virus, virus cũng chiếm một vùng bộ nhớ và sửa dịch vụ của hệ điều hành để khi đặt vào một đĩa khác, dịch vụ này sẽ gắn virus đang để trong bộ nhớ vào boot của đĩa mới và hoàn thành 1 chu kỳ lây lan.

SÂU (WORM)

- Sâu (worm) là chương trình hoàn chỉnh, không cần ký sinh vào boot hoặc file mà thông qua mạng (web hoặc mail) để nhân bản và phát tán. Vì sử dụng mạng nên tốc độ lây lan của sâu rất lớn
- Một số sâu phát tán qua email. Khi xâm nhập vào máy, nó tìm các địa chỉ email và tạo các thư điện tử gửi tới các địa chỉ đó có đính kèm các file là mã virus. Người nhận thư không biết mở file là bị nhiễm.
- Một số sâu được đặt trong các địa chỉ có thể download được dưới những lời giới thiệu có tính kích thích, để người dùng lấy về chạy thử và bị lây nhiễm

TẤN CÔNG TỪ CHỐI DỊCH VỤ (DOS)

DOS (Denial of Service) là loại hình tấn công khiến hệ thống không thể đáp ứng được yêu cầu dịch vụ nữa. Có 2 hình thái tấn công chính :

- Tiêu hao tài nguyên tính toán (như băng thông đường truyền, không gian đĩa, chiếm dụng thời gian CPU).
- Phá vỡ thông tin cấu hình của hệ thống khiến hệ thống từ chỗi dịch vụ (chẳng hạn làm sai lạc hệ thống DNS)

MẠO DANH, XÂM NHẬP TRÁI PHÉP

- Ăn cắp mật khẩu bảng cách thử tự động một cách có hệ thống
- Ăn trộm mật khẩu bằng cách bắt các gói tin của mạng để phân tích.
- Dùng các phần mềm gián điệp (Spyware). Phần mềm được gửi qua mail hay kích thích để người sử dụng download về chạy thử. Khi chạy một lần là bị nhiễm. Phần mềm này sẽ gửi các thông tin của máy ra ngoài giúp cho tin tặc có thể khống chế được máy bị nhiễm.
- Một loại phần mềm spyware là Keylogger, phần mềm loại này sẽ ghi lại các hoạt động của bàn phím đã gõ để gửi ra ngoài.
- Một khi đã khống chế được máy tính, tin tặc có thể lấy cắp thông tin, phá huỷ hay sửa chữa dữ liệu.

SỬ DỤNG MẠNG MÁY TÍNH VÌ CÁC MỤC ĐÍCH XẤU

- Phát tán các tài liệu văn hoá đồi truỵ, các tài liệu có hại cho an ninh, các tài liệu kích động các vấn đề dân tộc hẹp hòi, xung đột tôn giáo và bạo lực
- Lừa đảo tài chính qua mạng
- Đe doạ, quấy rối, đưa tin thất thiệt, xúc phạm người khác qua mạng

SỞ HỮU TRÍ TUỆ

- Bản quyền phần mềm: quyền tác giả, quyền sở hữu (quyền thương mại), quyền sử dụng
- Việt Nam đã tham gia công ước Bern về sở hữu trí tuệ
- Việc tôn trọng bản quyền phần mềm góp phần phát triển ngành công nghiệp phần mềm

MỘT SỐ ĐIỀU KHOẢN TRONG BỘ LUẬT HÌNH SỰ VỀ TỘI PHẠM TIN HỌC

- Điều 224. Tội tạo ra và lan truyền, phát tán các chương trình virus
- Điều 225. Tội vi phạm các quy định về vận hành, khai thác và sử dụng mạng máy tính điện tử
- Điều 226. Tội sử dụng trái phép thông tin trên mạng và trong máy tính
- Nghị định 55/2001/NĐ-CP, điều 41 quy định một số mức xử phạt các vi phạm khi sử dụng Internet chưa đến mức hình sự
  - Khoản 2 về Sử dụng mật khẩu, khoá mật mã, thông tin riêng của người khác để truy nhập, sử dụng dịch vụ Internet trái phép và sử dụng các công cụ phần mềm để truy nhập, sử dụng dịch vụ Internet trái phép"
  - Khoản 5 về Sử dụng Internet để nhằm mục đích đe doạ, quấy rối, xúc phạm đế danh dự , nhân phẩm của người khác; Đưa vào Internet hoặc lợi dụng Internet để truyền bá các thông tin, hình ảnh đồi truy, hoặc những thông tin khác trái với quy định của pháp luật về nội dung thông tin trên Internet; Đánh cắp mật khẩu, khoá mật mã, thông tin riêng của tổ chức, cá nhân và phổ biến cho người khác sử dụng; Vi phạm các quy định về vận hành, khai thác và sử dụng máy tính gây rối loạn hoạt động, phong toả hoặc làm biến dạng, làm huỷ hoại các dữ liệu trên Internet
  - Khoản 6 về tạo ra và cố ý lan truyền, phát tán các chương trình vi rút trên Internet

TỔNG KẾT

Các hoạt động có mục đích xấu liên quan đên CNTT bao gồm

- Tạo và reo rắc virus
- Xâm nhập trái phép chiếm đoạt thông tin, làm biến dạng hoặc huỷ hoại dữ liệu
- Vi phạm các quy định về vận hành, khai thác và sử dụng máy tính gây rối loạn hoạt động, phong toả hoạt động của máy tính và các hệ thống máy tính
- Lạm dụng mạng máy tính để thực hiện các tội ác khác như truyền bá thông tin có hại, xúc phạm cá nhân,, lừa đảo
- Vi phạm sự riêng tư
- Vi phạm bản quyền
- Pháp luật của Việt Nam đã có những quy định để trừng phạt những hành vi kể trên trong bộ luật hình sự và nghị định 55/2001/NĐ-CP. Tuy nhiên điều quan trọng là mỗi cá nhân phải nhận thức được trách nhiệm của mình trước cộng đồng

CÂU HỎI VÀ BÀI TẬP

- Thế nào là virus và worm và các phương thức hoạt động của nó
- Thế nào là tấn công từ chối dịch vụ.
- Nêu các khía cạnh của bản quyền phần mềm: quyền tác giả, quyền sở hữu và quyền sử dụng

CẢM ƠN ĐÃ THEO DÕI

HẾT BÀI 10. HỎI VÀ ĐÁP