Mã độc

Chương 8. Phòng chống mã độc

Mục tiêu

- Giới thiệu một số biện pháp phòng chống mã độc

Tài liệu tham khảo

[1] TS. Lương Thế Dũng, KS. Hoàng Thanh Nam, 2013, Giáo trình Mã độc, Học viện kỹ thuật Mật mã

Nội dung

1. Xây dựng chính sách phòng chống mã độc
2. Nâng cao nhận thức
3. Quản lý các lỗ hổng
4. Triển khai các công nghệ phòng chống mã độc

Nội dung

1. Xây dựng chính sách phòng chống mã độc
2. Nâng cao nhận thức
3. Quản lý các lỗ hổng
4. Triển khai các công nghệ phòng chống mã độc

Chính sách phòng chống mã độc

❑ Yêu cầu dùng phần mềm quét các thiết bị lưu trữ của các đơn vị bên ngoài tổ chức trước khi sử dụng.

❑ Yêu cầu những tập tin đính kèm trong thư điện tử, bao gồm cả các tập tin nén như file .zip cần được lưu vào ổ đĩa và kiểm tra trước khi được mở ra.

❑ Cấm gửi hoặc nhận một số loại tập tin có các đuôi tệp tin là exe qua thư điện tử.

Chính sách phòng chống mã độc

- ❑ Hạn chế hoặc cấm việc sử dụng phần mềm không cần thiết, ví dụ như các ứng dụng những dịch vụ không cần thiết hoặc các phần mềm được cung cấp bởi các tổ chức không rõ nguồn gốc.
- ❑ Hạn chế cung cấp quyền quản trị cho người sử dụng
- ❑ Yêu cầu luôn cập nhật phần mềm, các bản vá, cho hệ điều hành.

7

Chính sách phòng chống mã độc

- ❑ Hạn chế sử dụng các thiết bị di động (ví dụ: đĩa mềm, đĩa CD, USB), đặc biệt là trên hệ thống có nguy cơ ảnh hưởng cao, như các điểm truy cập công cộng.
- ❑ Yêu cầu nêu rõ các loại phần mềm phòng chống mã độc đối với từng hệ thống và các ứng dụng.

8

Chính sách phòng chống mã độc

- ❑ Người dùng nếu muốn có quyền truy cập vào các mạng khác (bao gồm cả Internet) cần thông qua sự đồng ý của tổ chức.
- ❑ Yêu cầu thay đổi cấu hình tường lửa để phù hợp với chính sách công ty
- ❑ Hạn chế việc sử dụng các thiết bị di động trên các mạng tin cậy.

9

Nội dung

1. Xây dựng chính sách phòng chống mã độc
2. Nâng cao nhận thức
3. Quản lý các lỗ hổng
4. Triển khai các công nghệ phòng chống mã độc

10

Nâng cao nhận thức

- ❑ Hướng dẫn cho các cán bộ, nhân viên cách phòng tránh sự cố liên quan đến mã độc hại, giảm thiểu mức độ nghiêm trọng của sự cố.
- ❑ Tất cả cán bộ, nhân viên trong tổ chức đều phải được đào tạo về các nguy cơ, cách thức phần mềm độc hại xâm nhập vào hệ thống, lây nhiễm, lây lan.

11

Nâng cao nhận thức

Không thực hiện một số công việc như sau:

- ❑ Không truy cập vào những trang web có khả năng chứa nội dung độc hại.
- ❑ Không mở các tập tin với phần mở rộng có khả năng kết hợp với phần mềm độc hại (Ví dụ: .bat, .exe, .pif, .vbs...).

12

Nâng cao nhận thức

Không thực hiện một số công việc như sau:

- **Không mở những thư điện tử hoặc tập tin đính kèm từ những địa chỉ của người gửi không rõ ràng hoặc có dấu hiệu nghi ngờ.**
- **Không truy cập vào các popup trên trình duyệt mà cảm thấy nghi ngờ hoặc có dấu hiệu bất thường.**

13

Nâng cao nhận thức

Một số khuyến cáo:

- **Không trả lời các thư điện tử yêu cầu cung cấp các thông tin tài chính và thông tin cá nhân.**
- **Không cung cấp mật khẩu, mã PIN hoặc các loại mã truy cập khác để trả lời thư điện tử hay điền thông tin vào popup hiển thị không mong muốn. Chỉ nhập thông tin vào các trang web chính thống của tổ chức.**

14

Nâng cao nhận thức

Một số khuyến cáo:

- **Không mở các tập tin đính kèm đáng ngờ trong email, thậm chí nếu những email này đến từ những người gửi đã biết.**
- **Không trả lời bất kỳ email nào đáng ngờ hoặc không mong muốn.**

15

Nội dung

1. **Xây dựng chính sách phòng chống mã độc**
2. **Nâng cao nhận thức**
3. **Quản lý các lỗ hổng**
4. **Triển khai các công nghệ phòng chống mã độc**

16

Nội dung

- **Quản lý bản vá**
- **Đặc quyền tối thiểu**
- **Biện pháp hỗ trợ khác**

17

Nội dung

- **Quản lý bản vá**
- **Đặc quyền tối thiểu**
- **Biện pháp hỗ trợ khác**

18

Biện pháp hỗ trợ khác

- Vô hiệu hóa, gỡ bỏ những dịch vụ không cần thiết.
- Loại bỏ những tập tin chia sẻ không đảm bảo.
- Sử dụng những tên đăng nhập và mật khẩu phức tạp phù hợp với chính sách của công ty.
- Yêu cầu xác thực trước khi cho phép truy cập vào dịch vụ mạng.
- Vô hiệu hoá cơ chế tự động thực thi các tệp tin nhị phân và các tệp tin scripts.

19

Nội dung

1. Xây dựng chính sách phòng chống mã độc
2. Nâng cao nhận thức
3. Quản lý các lỗ hổng
4. Triển khai các công nghệ phòng chống mã độc

20

Triển khai các công nghệ phòng chống mã độc

- Phần mềm Anti virus
- Phát hiện phần mềm gián điệp
- Ngăn ngừa sự xâm nhập hệ thống (IDS)
- Tường lửa

21

Phần mềm Anti virus

Một số phần mềm AV phổ biến

22

Phần mềm Anti virus

Các phương pháp phát hiện

- Phát hiện dựa trên dấu hiệu (signature based),
- Phát hiện dựa trên hành vi (behavior-based)
- Phát hiện dựa trên các dấu hiệu đặc biệt (specification-based)

23

Các phương pháp phát hiện

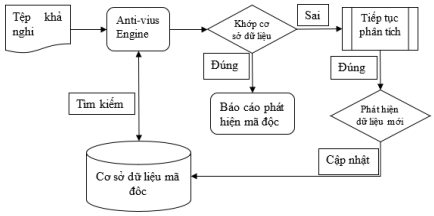
Phát hiện dựa trên dấu hiệu (signature based)

- Cơ sở dữ liệu mã nhận dạng
- Mã nhận dạng là một đoạn mã đặc biệt nằm trong tệp tin thực thi mà dựa vào đó có thể phân biệt được nó và các tệp tin khác

24

Các phương pháp phát hiện

Phát hiện dựa trên dấu hiệu (signature based)



Các phương pháp phát hiện

Phát hiện dựa trên hành vi (behavior-based)

- **Phân tích hành vi của các mẫu mã độc đã hoặc chưa biết**
- **2 pha chính: Pha đào tạo và pha phát hiện**

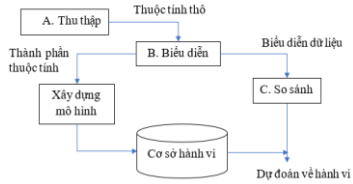
Các phương pháp phát hiện

Phát hiện dựa trên hành vi (behavior-based)

- **Trong pha đào tạo, hành vi của hệ thống sẽ được ghi nhận khi không có các cuộc tấn công và kỹ thuật học máy được sử dụng để tạo ra mẫu về hành vi bình thường.**
- **Trong pha phát hiện, mẫu về hành vi bình thường sẽ được so sánh với các hành vi hiện tại, sự khác nhau giữa chúng sẽ được đánh dấu là một cuộc tấn công.**

Các phương pháp phát hiện

Phát hiện dựa trên hành vi (behavior-based)



Các phương pháp phát hiện

Phát hiện dựa trên các dấu hiệu đặc biệt

- **Phát triển hệ thống nhận diện dựa trên hành vi để giảm khả năng phát hiện nhầm.**
- **Tập trung vào việc giám sát hoạt động của một chương trình và đánh hành vi của chương trình đó hơn là phát hiện dựa trên các cách tấn công đặc biệt.**
- **Có thể phát hiện mã độc đã và chưa biết và giảm việc phát hiện nhầm**
- **Tỉ lệ không phát hiện được mã độc vẫn cao**

Triển khai

Hai loại AV

- **Cho công ty (server client).**
- **Từng máy riêng biệt.**

Nội dung

1. Xây dựng chính sách phòng chống mã độc
2. Nâng cao nhận thức
3. Quản lý các lỗ hổng
4. Triển khai các công nghệ phòng chống mã độc