Tìm hiểu về tấn công Man In The Middle và Cách phòng tránh

Man In The Middle *hay MITM là phương thức tin tặc đặt mình vào giữa người dùng và ứng dụng. Nhờ đó tin tặc có thể nghe trộm hoặc đánh cắp thông tin nhạy cảm của người dùng. Do đó đây là một vấn đề bảo mật cần mà mọi người cần phải biết cách phòng tránh. Cùng NTT-Super365 tìm hiểu rõ hơn các hình thức tấn công và cách phòng chống trong bài viết này nhé.*

1. Những phương thức Man In the Middle Attack phổ biến

- **Wi-Fi eavesdropping**: Tin tặc sẽ thiết lập một kết nối Wi-Fi tại một địa điểm công cộng nào đó. Khi có người dùng kết nối vào mạng Wi-Fi sẽ thực hiện tấn công **man in the middle**. Nhằm theo dõi những hoạt động truy cập mạng của người dùng để ăn cắp thông tin dữ liệu.
- **Email hijacking**: Mục tiêu chính của phương thức tấn công này thường là các ngân hàng hoặc những tổ chức tài chính. Khi tin tặc chiếm được quyền truy cập sẽ giám sát được mọi giao dịch của tổ chức với khách hàng.
- **Stealing browser cookies**: Cookie trình duyệt là một phần thông tin nhỏ khi người dùng truy cập vào trang web. Những thông tin này sẽ được lưu trữ trên máy tính của bạn. Do đó tin tặc sẽ thực hiện **man in the middle** attack nhằm đáp cắp những dữ liệu này của bạn.
- **HTTPS spoofing**: Những website sử dụng giao thức truy cập HTTPS sẽ an toàn và có thể tin cậy được. Nhưng tin tặc có thể đánh lừa trình duyệt của bạn tin rằng nó đang truy cập vào một trang web an toàn. Từ đó thực hiện tấn công nhằm đánh cắp mọi thông tin hoạt động bạn với website.
- **DNS spoofing**: Kẻ tấn công giả mạo DNS bằng cách thay đổi địa chỉ của website trong máy chủ DNS. Khi người dùng truy cập website giả mạo này sẽ bị tấn công **man in the middle**. Từ đó có thể tăng lưu lượng truy cập website giả mạo của tin tặc nhằm đánh cắp thông tin đăng nhập của người dùng.

Man in the middle
Image not found or type unknown

2. Biện pháp ngăn chặn tấn công Man In The Middle

Tin tặc có thể sử dụng nhiều biện pháp khác nhau để tấn công MITM vào thiết bị của người dùng. Cho nên chúng ta nên chủ động phòng ngừa bằng những biện pháp sau:

- Cài đặt phần mềm phòng chống virus cho thiết bị cá nhân của bạn. Việc này giúp tránh các cuộc tấn công trung gian dựa trên các lỗ hổng bảo mật hoặc phần mềm độc hại.
- Hạn chế truy cập các điểm WiFi công cộng khi chúng không được bảo vệ bằng mật khẩu.
- Khi sử dụng máy tính công cộng nên đăng xuất tài khoản các nhân của bạn khi đã sử dụng xong.
- Sử dụng đăng nhập xác thực nhiều yếu tố và xoá đăng nhập các thiết bị không còn sử dụng.
- Chỉ truy cập sử dụng các trang web có giao thức HTTPS. Và nên đảm bảo rằng bạn luôn ở trang có ‘ổ khóa’ khi bạn cung cấp bất cứ dữ liệu nào.
- Sử dụng mạng riêng ảo VPN khi thực hiện các giao dịch và liên lạc quan trọng.
- Cảnh giác với các email lừa đảo từ nguồn không đáng tin cậy. Không truy cập vào bất cứ tệp tin đính kèm hay link nào đó có ở trong email.

*Mong răng bài viết này đã giúp bạn hiểu hơn về cuộc tấn cộng mạng **Man In The Middle***

https://www.youtube.com/embed/WwLiavkdcQY

Revision #1
Created 30 June 2023 09:14:32 by Quản trị
Updated 30 June 2023 09:17:24 by Quản trị