Module 9
Social Engineering

Những Nội Dung Chính Trong Chương Này

Social Engineering Là Gì ?
Human-Based Social Engineering
Computer-Based Social Engineering
Physical Attack
Inside Attack
Identity Theft
Online Scam
URL Obfuscation
Phòng Chống Social Engineering

Social Engineering Là Gì ?

Bên cạnh các biện pháp tấn công bằng kỹ thuật như sử dụng các chương trình tấn công thì hacker thường vận dụng kết hợp với các phương pháp phi kỹ thuật, tận dụng các kiến thức và kỹ năng xã hội để đạt được kết quả nhanh chóng và hiệu quả hơn. Và phương pháp tấn công không dựa trên các kỹ thuật hay công cụ thuần túy này được gọi là Social Engineering, trong đời thực thì dạng tấn công này có thể xem như là các kiểu lừa đảo để chiến dụng tài sản, giả mạo để đạt được một mục tiêu nào đó.

Có một câu chuyện thường được nhắc như là một dạng tấn công Social Engineering điển hình như sau " trong một cuộc thăm dò tính bảo mật và sự chặt chẽ trong quản lý thông tin của các công ty tại một cao ốc văn phòng lớn tại Wall Street, các chuyên gia bảo mật đã giả dạng một nhóm các chuyên viên an ninh mạng tiến hành một đợt khảo sát và thẩm định an ninh miễn phí cho các doanh nghiệp thuộc tòa cao ốc trên. Và trong đợt thử nghiệm này các "chuyên gia bảo mật giả dạng" đã yêu cầu nhân viên quản trị hệ thống của các doanh nghiệp cho phép kiểm tra các hệ thống máy chủ, kế cả những thông tin quan trọng để đánh giá xem có lổ hỗng nào hay không. Và kết quả thật đáng ngạc nhiên, có đến 7/10 công ty được yêu cầu đã cho phép các hacker trên thâm nhập và thao tác trực tiếp trên hệ thống của mình. May mà đây chỉ là các hacker mũ trắng đang hoạt động với mục tiêu đó lường tính bảo mật của doanh nghiệp.

Tại Sao Các Dạng Tấn Công Social Engineering Thành Công ?

Các hacker khi tiến hành các cuộc tấn công Social Engineering thường tận dụng những mối quan hệ thân thiết, tin cậy mà trong môi trường thông tin được gọi là các "trust relationship" để tiến hành khai thác mục tiêu. Chắc hẳn các bạn còn nhớ vụ Tiến Sĩ Lê Đăng Doanh bị hacker đắnh cắp hộp thư và gởi mail cho tất cả đồng nghiệp, bạn bè trong danh bạ để hỏi mượn tiền do đang bị kẹt tại nước ngoài. Hay chúng ta cũng thường xuyên nhận tin nhắn từ các số máy lạ để yêu cầu mua giùm một thẻ điện thoại rồi gởi mã số đến số của hacker.

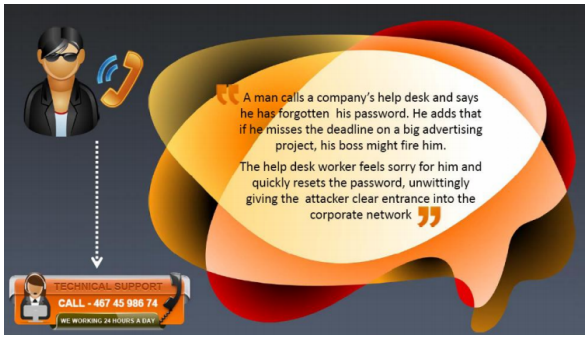
Việ tấn công này rất hiệu quả vì đánh vào điểm yếu nhất trong quy trình an toàn thông tin của chúng ta, đó là sự kém hiểu biết của người dùng. Chính vì vậy để phòng chống các dạng tấn công này thì doanh nghiệp cần có những chương trình đào tạo nhăm nâng cao nhận thức an toàn thông tin cho nhân viên của mình.

Những Kiểu Tân Công Thông Dụng Của Social Engineering

Social Engineering được chia làm hai hình thức chính :

> **Human-based** : Human-based social engineerign dựa trên dựa trên mối qua hệ giữa người – và – người để khai thác, thu thập thông tin như gởi điện thoại hỏi các nhân viên bộ phận hỗ trợ người dùng để thử tìm các thông tin nhạy cảm.
>
> **Computer-based** : Computer-based Social Engineering sử dụng các chương trình máy tính hay những trang web để dẫn dụ người dùng nhập vào các thông tin bí mật là tài khoản và mật khẩu truy cập. Dạng tấn công này thường được gọi là phissing.

Human-Based Social Engineering



Những trường hợp điển hình cho dạng tấn công này là giả dạng nhân viên hay là cộng tác viên để truy cập vật lý vào những thông tin được bảo vệ. Như giả dạng làm nhân viên bảo trì hệ thống để đột nhập phòng máy chủ trái phép. Bên cạnh đó hacker còn giả làm một nhân vật quan trọng hay nhân vật thứ ba nào đó để gọi điện thoại cho bộ phận hỗ trợ, những quản trị hệ thống yêu cầu cung cấp các tài khoản quản trị như hình minh họa. Tình huống tấn công này đã được hacker Kevin Mitnick cùng cộng sự trình diễn tại đại hội Blackhat, trong tình huống này anh ta đã dùng phần mềm giả giọng nói và cả số điện thoại của một nhân vật quản trị cao cấp yêu cầu quản trị mạng nhắc mật khẩu email do bị quên password, và kết quả là hoàn toàn thành công.

Shoulder surfing : Dạng tấn công này hacker sẽ xem lén thông tin mật khẩu chúng ta nhập vào màn hình như tên tài khoản, xem lén kí tự bàn phím hay lắng nghe các âm thanh phát ra khi người dùng gõ vào để đoán xem đó là những kí tự gì. Vì lý do này mà nhiều doanh nghiệp cho thiết kế các trạm làm việc sao cho vẫn bảo đảm tính thận thiện nhưng ngăn ngừa người này có thể nhìn thấy màn hình của người khác.

Dumpster diving : Cũng có những tình huống các hacker giả dạng làm những người quét dọn vệ sinh, hay những đồng nghiệp lục lọi hồ sơ của nhau để tìm kiếm các bị mật công nghệ, nhưng thông tin riêng tư và hình thức này được gọi là Dumpster diving. Vì vậy, các doanh nghiệp thường trang bị các máy hủy giấy để ngăn ngừa các thông tin bí mật hay các ý tưởng quan trọng bị lộ từ các mãnh giấy bỏ. Hoặc chính sách của các công ty này yêu cầu nhân viên khi rời khỏi bàn làm việc phải đặt màn hình chế độ Screen Saver, và lật úp mặt các tài liệu mang tính riêng tư của mình.

Một hình thức nâng cao khác của social engineering là *reverse social engineering*, trong tình huống này hacker sẽ giả mạo những người có đủ thẩm quyền để truy cập thông tin mật, hay giả vờ đóng vai trò những chuyên viên hỗ trợ để dò hỏi các tài khoản của người dùng như trong ví dụ mà ta thấy ở phần trên.

Computer-Based Social Engineering

Dạng tấn công *computer-based social engineering* bao gồm :

- E-mail attachment / Phising
- Fake website

└ Popup window

Hàng ngày chúng ta nhận rất nhiều email lừa đảo hay còn gọi là phising mail với những thông tin hấp dẫn như các bạn vừa trúng một giải thưởng lớn như Hình 9.1, hay được gởi tặng thiệp điện tử những hình ảnh qua mail đính kèm, hay liên kết dẫn đến trang web để người dùng nhấn vào có khả năng bị lây nhiễm virus, hoặc dẫn đến các trang web nguy hiểm chứa mã độc.

Hình 9.1 - Một thông điệp giả mạo thường thấy trên email

Đôi khi các trang web được làm giống như những trang chính thức như Paypal, Ebay, Clickbank … để khi chúng ta đăng nhập sẽ bị đánh cắp thông tin. Các trang web giả mạo như vậy gọi là Fake Web, một dạng tấn công điển hình của Computer-based Social Engineering. Ngoài ra, các trang web nguy hiểm còn tạo các cữa sổ popup với các thông tin cảnh báo người dùng bị virus, hay máy tính của bạn đã bị nhiễm một loại virus, yêu câu tải về một chương trình để quét và dĩ nhiên đây là chương trình nguy hiểm.

Tấn Công Vật Lý Và Tấn Công Từ Bên Trong

Bảo vệ thông tin ở mức vật lý là một trong những mục tiêu quan trọng hàng đầu của an toàn thông tin. Vì vậy nhiều tổ chức hay doanh nghiệp xây dựng các phòng máy chủ với hệ thống an ninh nhằm bảo vệ sự an toàn tối đa cho những thiết bị quan trọng. Việc bảo vệ các thiết bị vật lý ngoài phòng chống mất cắp hay ngăn không cho kẻ gian xâm nhập và tương tác vào các thiết bị quan trọng chúng ta cần có những hệ thống bảo đảm sự ổn định điệp áp, giữ nhiệt độ phòng ở mức thích hợp cho sự vận hành của các máy chủ, phòng chống cháy nổ theo các chính sách an ninh cần được tuân thủ đầy đủ.

Đối với những máy trạm hay hệ thống máy tính của nhân viên, việc bảo đảm an toàn vật lý sẽ ngăn ngừa các hacker lấy trộm thông tin thông qua các giao tiếp USB, cài đặt các chương trình nguy hiểm và đề phòng mật cắp máy tính xách tay vì đây là những mục tiêu mà hacker hay kẻ gian thường nhắm đến. Những hình thức như vậy thuộc dạng tấn công ở mức vật lý.

Nếu một hacker không tìm được cách nào để tấn công vào mục tiêu từ bên ngoài thì họ sẽ tấn công từ bên trong, đây chính là *insider attack* một giải pháp tấn công hiệu quả mà các chuyên gia phòng chống tội phạm cũng thường sử dụng. Insider Attack ngụ ý các hacker trà trộn hay thâm nhập vào nội bộ của công ty, tổ chức bằng cách xin làm nhân viên của doanh nghiệp để tận dụng lợi thế từ bên trong và tiến hành các thao tác đánh cắp dữ liệu dễ dàng hơn. Vì vậy

có câu nói " nếu bạn ở bên trong, bạn sẽ là chủ nhân của hệ thống mạng". Đây cũng là một tình huống thuộc dạng tấn công vật lý.

Chúng ta dễ dàng nhìn thấy các tình huống tương tự trong các phim ảnh hành động mà ở đó các gián điệp được cài cắm vào hàng ngũ cổ kẽ địch hay các tổ chức tội phạm để điều tra manh mối. Một ví dụ điển hình đó là tổ chức hacker khét tiếng hiện nay Anonymous đã bị chính các nhân viên anh ninh của FBI trà trộn vào hàng ngũ của mình,sau đó lần ra các manh mối và danh tính của những thành viên quan trọng trong tổ chức "ẩn danh" này, làm cho hơn 25 thành viên chủ chốt đã bị bắt giam trong đó có cả thủ lĩnh mang biệt danh Sector404.

Hình 9.2 - Một thành viên của tổ chức hacker Anonymous

Identity Theft

Identuty Theft nói đến việc đánh cắp định danh của người dùng bao gồm từ việc ăn trộm mật khẩu email, tài khoản ngân hàng cho đến việc lấy cắp các thẻ kiểm tra an ninh để đột nhập vào những khu vực được bảo vệ.

Online Scam

Một số trang web đưa ra các thông tin giả mạo để dẫn dụ người dùng nhập vào địa chỉ email và mật khẩu. Như các tình huống hacker gởi link chưa hình ảnh qua Yahoo ! Messenger và khi chúng ta click vào sẽ được dẫn đến một trang web yêu cầu nhập vào email và password của hộp thư Yahoo để có thể xem hình ảnh này, rõ ràng đây là các trang web Fake (website giả mạo, lừa đảo) nên khi chúng ta nhập thông tin vào sẽ bị các hacker đánh cắp.

Hình thức này còn xảy ra khi hacker gởi những email có chưa mã độc được nhúng trong tập tin đính kèm, các chương trình nguy hiểm này có thể là virus, trojan hay key logger đánh cắp các thông tin mà chúng ta nhập vào từ bàn phím. Như trong ví dụ sau sẽ minh họa về một email scam có chứa các chương trình nguy hiểm trong tập tin đính kèm.

Mail server report.
Our firewall determined the e-mails containing worm copies are being sent from your computer.
Nowadays it happens from many computers, because this is a new virus type (Network Worms).
Using the new bug in the Windows, these viruses infect the computer unnoticeably.
After the penetrating into the computer the virus harvests all the e-mail addresses and sends the copies of itself to these e-mail addresses
Please install updates for worm elimination and your computer restoring.
Best regards,
Customer support service

Nội dung thông điệp này tương tự như nhiều email lừa đảo khác yêu cầu người dùng thay đổi tên và mật khẩu truy cập vào các tài khoản quan trọng Paypal, E-gold … mà chúng ta vẫn thường nhận được. Bên cạnh hình thức Email Attachment thì một số trang web đen hay hiển thị những Popup (cữa sổ) cảnh báo chúng ta bị nhiễm virus, hay bạn vừa có một email mới để khi nhấp vào thì sẽ được chuyển hướng đến một trang web khác chưa những nội dung nguy hiểm hay các trang web quảng cáo.

URL Obfuscation

URL là Uniform Resource Locator thường được nhập vào trình duyệt để kết nối đến các trang web. Và thay vì đưa ra đường dẫn đến trang web mà người dùng cần truy cập thì các hacker sẽ cố tình thay đổi các đường dẫn url này đến một trang web giả mạo khác để lấy cắp thông tin mà người dùng không nhận ra do các liên kết này thường được ẩn dưới dạng một hyper link trong các tập tin word hay pdf, đây là hình thức tấn công theo kiểu URL Obfuscation.

Phòng Chống Social Engineering Như Thế Nào ?

Để phòng chống bị tấn công Social Engineering chúng ta cần nâng cao nhận thức và kiến thức về an toàn thông tin cho người sử dụng thông qua các buổi huấn luyện và các chương trình đào tạo.

Bên cạnh đó, trong mỗi tổ chức cần có một chính sách an ninh chặt chẽ kết hợp với những biện pháp chế tài để hạn chế và ngăn ngừa những hành vi xâm phạm thông tin trái phép. Chính vì lý do này mà trong các mô hình phòng thủ theo chiều sâu để bảo vệ thông tin thì lớp chính sách bảo mật luôn được nhấn mạnh và bao trùm lên tất cả các lớp phòng thủ vật lý khác, đồng thời quá trình huấn luyện người dùng được xem như là hành động quan trọng hàng đầu trong công tác bảo vệ an toàn thông tin.

Ngoài việc bảo vệ các dữ liệu thì chúng ta cần bảo vệ các thiết bị lưu trữ, vận hành hệ thống thông tin như đĩa cứng, máy chủ, hệ thống truyền dẫn như cáp truyền, mạng wifi nhằm tránh sự tương tác trực tiếp của hacker. Một trong các phương pháp để bảo vệ vật lý là ngăn không cho sự xâm nhập trái phép với những thông báo như “không phận sự miễn vào” , đề ra chính sách sử dụng thiết bị thích hợp phòng bị mất mát dữ liệu qua các đường truyền internet, đường kết nối dial-up hay ổ cắm USB. Và cũng cần lưu ý, những nhân viên của công ty hay

những người làm việc bán thời gian đều có thể là những hacker nguy hiểm có khả năng tấn công vật lý vào hệ thống.

Bên cạnh những tác nhân con người, thì các yếu tố đến từ thiên nhiên như hỏa hoạn, động đất cũng là các yếu tố hàng đầu cho nguy cơ mất an toàn thông tin, như thảm họa 11/9 là một ví dụ điển hình. Do đó chúng ta cần có một kế hoạch bảo đảm tính liên tục và phục hồi thảm họa thông qua các giải pháp sao lưu, xây dựng các hệ thống dự phòng đáp ứng các yêu cầu của tổ chức. Và cuối cùng, những tác nhân đến từ môi trường như nguồn điện, nhiệt độ cũng có thể đem đến những mối nguy hiểm về mất mát thông tin do đó trong vai trò CEH chúng ta cần lưu ý đến những tác động này, cần có các hệ thống ổn định nguồn điện, hệ thống điện dự phòng, hệ thống điều hòa nhiệt độ. Thậm chí, nhiều doanh nghiệp còn ứng dụng quy luật phong thủy trong vấn đề sắp đặt từ vị trí workstation cho đến các máy tính, máy chủ nhằm đem đến sự hòa hợp giữa môi trường và cơ sở vật chất và tạo ra sự thuận lợi trong công việc kinh doanh.

Đây chính là những vấn đề mà các bạn cần chú ý trong chương Social Engineering và đề phòng tấn công vật lý.

Tổng Kết

Qua chương này chúng ta đã nắm một số khái niệm quan trọng như dạng tấn công Social engineering ứng dụng các kỹ năng xã hội, dùng mối quan hệ con người để thu thập tin cần thiết phục vụ cho những cuộc tấn công phía sau. Việc các cuộc tấn công social engineering có thể thành công là do đánh vào điểm yếu của con người. Các bước thực hiện một cuộc tấn công Social engineering gồm : Thu thập thông tin, chọn mục tiêu, tấn công. Ngoài ra, các bạn cũng đã tìm hiểu những vấn đề Insider Attack, Indentify Theft, Online Scam, Phising…

Và cuối cùng là để phòng chống lại kiểu tấn công này, chúng ta cần phải đào tạo, huấn luyện người dùng để nâng cao nhận thức về an toàn thông tin cho họ.