Автор: Цветелина Николова

СОЦИАЛНО ИНЖИНЕРСТВО

Основната цел на социалното инженерство е същата, като на хакерството: придобиването на неоторизиран достъп до системи или информация, с цел измама, кражба на идентичност, индустриален шпионаж, или причиняване на друга вреда.
Основната разлика е, че социалното инженерство използва главно психологически методи, а именно естествената за човека склонност да се доверява. Типичните цели на подобни атаки са телекомите, известни корпорации и финансови институции, военни и правителствени организации, болници.

Атаките на социалното инженерство протичат на две нива:
- Физическото ниво са офиси, телефони, кошчета за боклук, служебна поща.

На работното място социалният инженер може просто да влезе, представяйки се за лице по поддръжката, и да се разходи, докато намери няколко въргалящи се по бюрата пароли. Или незабелязано да наблюдава как усърден служител въвежда паролата си (shoulder surfing).
- Психологическият подход, използващ утвърдени методи за убеждаване: представяне за някой друг, конформизъм, позоваване на авторитетна фигура, разсейване на отговорността или просто дружелюбно отношение.

"**Hunting**" и "**Farming**" са два от най-често използваните методи, с които си служат кибер престъпниците, за да получат конфиденциални данни или директно да поискат „откуп" от атакуваните потребители. И при двата метода се разчита на т.нар. социално инженерство, като независимо дали жертвата е потребител, критична инфраструктура на организация или търговка верига, атакуващият разчита на способността си да убеди потребителя да предприеме действие, улесняващо заразяването със зловреден код.

При методът на „ловуването" (hunting) атакуващият се стреми да реализира бърза печалба, например, чрез заплахата CryptoLocker, чрез която редица компютри и бази данни бяха „заключени", а за ключът нападателят иска „откуп". Тази атака засегна и много компютри в България, но тъй като жертвите рядко съобщават за нея, дори в полицията, останаха неясни размерите на щетите у нас. При методът „обработка" (farming) стремежът на нападателите е да останат възможно най-дълго време скрити от потребителя и системите за защита, така че да се възползват продължителен период от време от информацията в компютъра или от неговите ресурси.

Хакерите, които си служат със социалното инженерство използват принципите на Чалдини за техниките на убеждаване и влияние:

1. Авторитет (симулира се нареждане, получено от разполагащ с власт над потребителя - – полиция, ФБР, понякога и висшестоящ шеф);

2. Харесване (измама тип „харесваме“, симпатизираме на един и същи неща – отбори, училищни сбирки);

3. Реципрочност (разчита се на реакцията на жертвата на изпратени „лични данни“ или друга интересна за нея информация, при която тя се чувства „задължена“ да сподели свои данни);

4. Consistency (Придържане към принципите);

5. Социално одобрение (най-често хората кликват върху спам, изпратен уж от приятел в социалните медии);

6. Scarcity (Недостиг или ограничено количество от желана от жертвата стока или услуга).

Кевин Митник, известен бивш хакер и основоположник на социалното инженерство, заключава: “много по-лесно е да подлъжеш някой да ти даде паролата за дадена система, отколкото да загубиш часове в усилия да я разбиеш”.

На една от последните DEF CON Hacking Conference, Social-Engineer.org са организирали състезание между участниците, в рамките на което всеки е можел да тества social engineering уменията си, опитвайки се да събере важна вътрешна информация от компании като Coca Cola, Shell, Ford, дори ИТ гиганти като Google, Microsoft, Apple, Cisco и други. Изненадващо, места се оказва доста успешен - представяйки се за журналисти, бизнесмени и IT специалисти, хакерите успяват да получат информация като спецификациите на проекти със затворен код или вида и версията на браузъра и антивирусния софтуер, използвани от служителите. Някои от участниците дори успяват да убедят отсрещната страна да посети URL, продиктувано по телефона.

Независимо от използвания метод, целта е жертвата да бъде убедена, че социалният инженер е човек, на когото може да има доверие при разкриването на поверителна информация.

Социалното инженерство е предпочитан метод, с който да се започне атака върху дадена система, защото при невнимание от страна на потребителя, атакуващият лесно може да получи необходимата информация.