Социално инженерство

Повечето сложни и успешни атаки не са свързани с техническо проникване в дадена система, а имат социален характер. Вместо да се използва технология за влизане в дадена система, социалното инженерство опитва да намери хора, които да изпълнят заявките на атакуващите. Това не означава, че вие можете отдалечено да контролирате техните мисли и намерения. Социалното инженерство използва навиците на хората по такъв начин, че те да не разберат, че някой е получил от тях някаква информация.

Повечето атаки се осъществяват, като хакера се представя за някой друг. Това разбира се включва повече от просто обаждане до IT отдела на дадена компания и поискване на паролите за компютрите, на които се намират защитния софтуер. Въпреки че може да не повярвате на това, всичко може да завърши само с един телефонен разговор, ако е подготвено добре.

Социалното инженерство акцентува върху най-слабата връзка при Интернет сигурността - човека. За да бъде защитена една система, тя не трябва да бъде свързана към Интернет. Но дори и това не може да гарантира, че системата наистина ще бъде сигурна. През април 1999 г. хакери успяха да откраднат информация от институт за ядрени изследвания в САЩ, като използваха вътрешен човек, който изкопира необходимата им информация върху дискета.

Много бизнес компании разчитат на Интернет, а в бъдеще почти всички компании ще искат да участват в Интернет бизнеса. От тук се вижда, че всяка една от тези компании може да се окаже цел за хакерите. Социалното нахлуване улеснява хакерите, тъй като то не зависи от платформата, от операционната система или от приложния софтуер на системата на хакера.

Социалното хакерство работи по индиректен начин. Всеки, който има връзка с хора, познаващи системата за защита на информацията на дадена компания, може да се разглежда като потенциален риск за сигурността. С едно обаждане на секретар могат да се разберат имената на хората, работещи в дадена организация, от които може да се получи допълнителна информация. След няколко телефонни разговора, които не могат да се проследят, така както могат да се проследят електронни пощи, хакера получава

достатъчно информация за компанията и нейните процедури на работа, така че просто може да се обади на някой от отдела по сигурност и да се представи за даден служител от компанията.

Събраната информация е като малки части от пъзел, които изглеждат съвсем незначителни за този, който предоставя информацията. Само че събрана като цяло, тази информация може да се използва за атаки срещу компанията. За да получи необходимата информация, необходимо е този, който я събира да се адаптира към вътрешните за компанията процеси. Схемите показващи структурата на компанията и телефонните указатели може да се окажат нещо доста полезно. Вътрешните документи, които се изхвърлят, винаги трябва да се късат, за да не може случаен минувач просто да си извади от кофата за боклук. Понастоящем използването на дискети трябва да се елиминира изцяло. Информацията от форматирана дискета може да се възстанови лесно. Твърдите дискове и дискетите, които вече не се използват в дадена компания трябва да се унищожават изцяло. Социалното инженерство не изисква задълбочени компютърни познания и дава възможност на всеки да се превърне в хакер.

Друг метод за получаване на информация е просто тя да се поиска директно. Просто можете да се обадите на администраторите и да поискате паролите за системата, обезпечаваща защитата на информацията. За да имате успех трябва да имате поглед върху структурата на компанията. Хакерът, например може да разбере, че някой мениджър на компанията, която смята да атакува е просто в друга държава, която е в часова зона различаваща се с осем часа от тази на държавата, в която е неговата компания. Да предположим, че този мениджър ще изнася реч в тази държава. Тогава хакерът може да се обади в офиса половин час преди речта на мениджъра и да попита за паролата, защото преносимия компютър, на който е презентацията не работи. Поради разликата в часовата зона, най-вероятно в държавата където е офиса на компанията да е нощ и само дежурните служители да бъдат на работа. Хакерът може да се представи за мениджъра и да поиска информацията да му бъде предоставена веднага, за да не закъснее със своята реч. За да убеди служителите, че той е този, за който се представя той може да поиска да говори с ръководителя на IT отдела.

Представете си този случай. Ако вие сте на мястото на този, от който се изисква да даде паролата ще го направите ли? През работно време може би ще направите някои проверки, но през нощта, когато сте сънен най-вероятно ще дадете исканата от вас информация без да се замислите. Социалното инженерство събира информация и оказва социален натиск. Една от често използваните стратегии е да се получи информация от служител, който очаква да бъде уволнен.

Хакерите използват силни аргументи когато правят последната стъпка от своята атака, тъй като слабите аргументи могат да породят съмнения. Когато се представят силни аргументи повечето хора се подчиняват. Този вариант ще има добър успех, особено ако човека, който се атакува е по-малко компетентен от хакера.

Както виждате, когато в администрирането на една система участва фактора човек, дори и тази система да има най-добрата защита, тя може да бъде атакувана индиректно. За да намалите верността вашата система да бъде атакувана посредством социално инженерство, трябва да обучите всички служители във вашата компания. Всеки един служител трябва да разбира важността на сигурността и да знае какви са методите използвани от хакерите. В много случаи е по-лесно да се получи информация от тези, които работят с компютрите, отколкото от самите компютри. В същото време е истина, че е по-лесно да се принудят служителите да не дават информация, отколкото да защитите даден компютър. Изводът от това е, че е необходимо непрекъснато обучение на служителите.