Mis on tehnosotsiaalne sahkerdamine ehk social engineering?

5. august 2014 - 23:11 Autor: Sten Mäses

Sotsiaalne sahkerdamine *(Social engineering*) on meetod, mille käigus kasutatakse infole või ressurssidele (nt IT-süsteemidele) omavolilise ligipääsu saamiseks erinevaid inimestega manipuleerimise tehnikaid. Oskusliku pettuse tõkestamine on üpriski keeruline, sest inimeste loomuses (ja sageli ka töökirjelduses) on olla abivalmis ja kuulekas. Seetõttu on isegi umbusklikul töötajal raske keelduda autoriteetse ja enesekindla häälega jagatud juhistest või hädasolija abipalvest. Mis see sotsiaalne sahkerdamine aga ikkagi täpsemalt on ja kuidas sellega kaasnevatest kurbadest tagajärgedest hoiduda?

Sotsiaalne mõjutamine

Teiste inimeste mõjutamine kui meetod oma eesmärkide saavutamiseks pärineb juba eelajaloolisest ajast, sest ilma üksteise mõjutamiseta on praktiliselt võimatu koostööd teha. Sotsiaalse sahkerdamise all on aga antud kontekstis mõeldud pigem omakasupüüdlikku manipulatsiooni, mis võimaldab saavutada vajaliku tulemuse lihtsa suhtluse abil. Küberturvalisuse kontekstis rõhutab social engineering võimalust inimeste manipuleerimise abil mööda hiilida tehnilistest turvameetmetest. Näiteks võib e-posti kontole ligipääsemiseks keeruka häkkimise asemel lihtsalt kasutajalt otse küsida. Kui õnnestub jätta mulje, et seda nõuab ülemus, politsei või keegi teine autoriteetne isik, siis ei ole sugugi välistatud, et kasutaja oma parooli näiteks telefonikõnes vabatahtlikult avaldab. Veel üks levinud võte personaalset informatsiooni välja petta on teenindava personali kaudu, kelle tööülesandeks on inimesi aidata. Hädasoleva kliendi või väidetava kolleegi aitamiseks võivad mitmed teenindajad kogemata manipulatiivsele ründajale konfidentsiaalset informatsiooni paljastada.

Tehnosotsiaalne sahkerdamine

Eriti tõhus (ja seetõttu ohtlik) on sotsiaalne mõjutamine, kui seda kombineerida tehnilise küberrünnakuga. Näiteks võib rünnatav arvutikasutaja keelduda oma kasutajanime ja parooli telefoni teel avalikustamast, kuid installib kuulekalt väidetava IT-toe poolt saadetava turvauuenduse, mis võib tegelikult olla viirus, klahvinuhk (keylogger) või muu pahavara. Tänapäevaste vabalt Internetis levitavate häkkimisvahenditega on lihtne luua vajalikust veebilehest suhteliselt täpne koopia, mis salamisi külastajate arvutitest turvaauke püüab leida. Vahel pole isegi turvaauku vaja leida, kui õnnestub rünnatavat kasutajat veenda oma isiklikke andmeid vabatahtlikult sisestama.

Tehnilisi ja sotsiaalseid oskusi meisterlikult kasutades suutis Kevin Mitnick, üks tuntumaid sotsiaalseid sahkerdajaid, kolm aastat FBI-ga kassi-hiirt mängida. Kui FBI agendid (enda meelest) ootamatult Mitnick'i korterit külastasid, leidsid nad külmkapist paki sõõrikuid pilkava sildiga "*FBI donuts.*" Mitnicki enda sõnul tegeles ta inimeste tüssamisega peamiselt enda lõbuks, mitte rahalistel eesmärkidel.

Aina rohkem on aga küberkriminaalid hakanud inimeste lihtsameelust ja abivalmidust kurjalt ära kasutama just sooviga - kas siis otseselt (nt inimestelt raha või hinnalist infot välja pettes) või kaudselt (nt konkurendi mainet kahjustades) - rikastuda. Kuna sotsiaalne sahkerdamine on oma olemuselt väga lihtne, siis on seda ennetada üpris keeruline. Näiteks pommiähvardusega saab hakkama isegi algkooli õpilane ja tegelikku ähvardust võltsist eraldada on praktiliselt võimatu. Kuidas siis ikkagi vähendada riski tehnosotsiaalse sahkerdamise ohvriks sattuda?

Sahkerdamisvastased abinõud

Tehnosotsiaalse sahkerdamise vastu tegutsemist tasub organisatsioonides alustada uutest töötajatest, sest just nemad on oma ebakindluse ja kogenematusega libekeelsete ründajate lemmiksihtrühm. Võimalikult varakult tuleks veenduda, et kõik töötajad on kursis organisatsiooni eeskirjade ja tavadega. Lisaks tuleks kõigile töötajatele selgeks teha, kuidas potentsiaalseid pettureid ära tunda ja mida sel juhul teha.

Näiteks tasub eriti ettevaatlik olla tundmatute inimestega, kellel on väga kiire. Hädaolukorra (vähemalt näilik) loomine takistab rünnataval isikul selge pilguga olukorda hinnata ja suurendab tõenäosust, et tegutsetakse mõtlematult petturi abistamiseks. Peaaegu alati on võimalik korraks aeg maha võtta ja pakilist probleemi rahulikult lahata. Abiks oleks kindlasti ka täpsed eeskirjad, mida erinevate hädaolukordade puhul tuleks järgida.

Teine märk, mis peaks koheselt valvsust suurendama, on salasõna küsimine. Professionaalne IT-töötaja, koristaja, naaber alumiselt korruselt, teller pangas ega keegi teine ei tohiks huvi tunda kellegi teise isikliku salasõna või koodi vastu.

Valvsust peaks koheselt suurendama ka e-kirjas sisalduv viide või manustatud fail. Kui e-kiri pärineb tuttavalt inimeselt, kuid selle sisu on vähimalgi määral ebatavaline, siis tasub võimaluse korral saatjaga (näiteks telefoni teel) ühendust võtta ja kontrollida, et kiri tõepoolest pärineb väidetavalt isikult.

Lisaks tehnilistele tulemüüridele ja viirusekaitseprogrammidele tasuks üle vaadata ka arvuti füüsiline kaitse. Näiteks pole sugugi välistatud, et suuremates organisatsioonides saab enesekindla olekuga kurikael sületäie sülearvutitega tähtsal ilmel asutuse peauksest välja marssida ilma, et keegi midagi kahtlustaks. Töökohas oma arvuti tagant lahkudes tasub see kindlasti lukustada. ASA Quality Services kontoris on näiteks selline kord, et järelvalveta ning lukustamata jäetud arvuti omanik toob kolleegidele maiustamiseks koogi. Säärased meetmed tekitavad ka uutes töötajates kiirelt harjumuse laua tagant lahkudes oma arvuti eeskirjade kohaselt lukustada.

Turvalisuse mitu kihti

Erinevate inimmanipulatsioonide vältimisel ei maksa aga unustada ka tavapärast turvarutiini. Mitmeastmeline autentimine ja korralik paroolihaldus aitavad võimaliku infolekke levimist tõkestada ning tarkvarauuendused takistavad laialdaselt teadaolevate turvaaukude ärakasutamist. Nii nagu maja ehitamisel ja korras hoidmisel tuleb tähelepanu pöörata igale seinale (ning meeles pidada ka vundamenti ja katust kontrollida), nii tasub ka küberturvalisuse puhul tähelepanu pöörata lisaks arvutitevahelist suhtlust kirjeldava OSI mudeli seitsmele suhtlustasandile ka kaheksandale – inimfaktorit sisaldavale kihile. Kõige tõhusam kaitse küberrünnakute vastu on terviklik turvapoliitika: lisaks tehniliste rünnete vältimisele tuleks hoiduda ka sotsiaalse sahkerdamise eest.

STEN MÄSES
ASA Quality Services
(artikkel on pärit ASA Quality Services blogist)

- Uudised
- Turvalisus