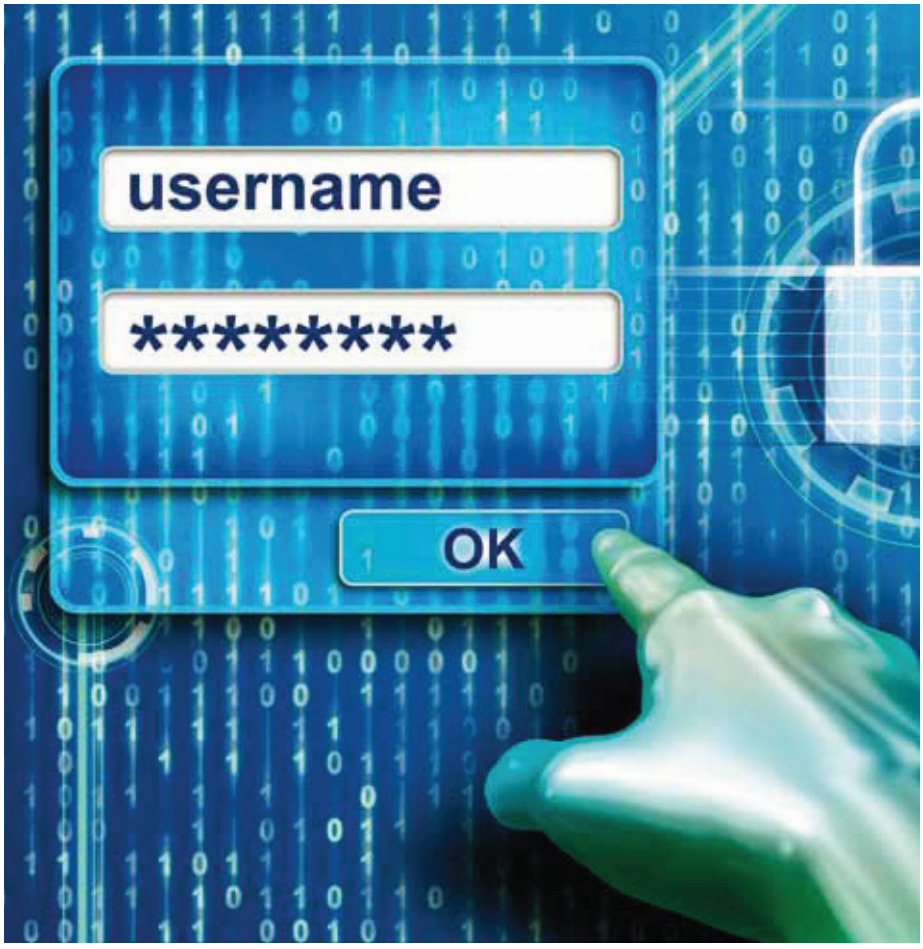
Enimark Ponjević, direktor poduzeća General Security, redovito odgovara na pitanja i savjetuje čitatelje Poslovnog savjetnika s aspekta sigurnosti i unaprjeđenja poslovanja

Socijalni inženjering i obmanjivanje sustava

Socijalni inženjering je akt manipulacije kojim se ljudi navode da odaju povjerljive informacije o sebi. Ta tehnika prevare zasniva se na ometanju pažnje određene osobe u cilju prikupljanja informacija koje ta osoba inače ne bi odala. Dobiveni podaci se kasnije zloupotrebljavaju radi saznavanja lozinki, korisničkog imena, podataka o kreditnim karticama itd.



Sve metode socijalnog inženjeringa temelje se na specifičnim pravilnostima u procesu donošenja odluka neke osobe. Napadač navodi žrtvu na „pogrešnu kogniciju“ koja predstavlja obrazac neispravnog prosuđivanja čovjeka u određenoj situaciji.

Spiskovi koji slijede ukratko opisuju metode obmane i postupke prevare kojima su svakodnevno izložene Vaše tvrtke. Prilagodite ove podatke svojoj organizaciji i dajte ih svim radnicima kako bi ih primijenili kada se ukaže problem sigurnosti informacija.

CIKLUS OBMANE

Ciklus obmane metodom socijalnog inženjeringa započinje istraživanjem i ispitivanjem podataka o žrtvi iz javnih izvora kao što su godišnji izvještaji, marketinške brošure, prijave patenata, isječci iz tiska, stručni časopisi i web lokacije, pa sve do kopanja po smeću.

Nakon toga napadač razvija dobre odnose i povjerenje uz upotrebu internih informacija, lažnog predstavljanja, spominjanja osoba koje žrtva poznaje, molbi za pomoć ili pozivanja na autoritet.

Tada slijedi faza zloupotrebe stečenog povjerenja te traženje informacija ili usluga od žrtve, a moguće je i manipuliranje žrtvom tako da sama zatraži pomoć od napadača.

Dobivenim informacijama napadač može nanijeti nesagledivu štetu Vašoj tvrtki ili instituciji, a da nikada niti ne postanete svjesni da ste žrtva socijalnog inženjeringa.

Uobičajene mete napada metodom socijalnog inženjeringa su žrtve koje nisu svjesne značaja informacija. U tu kategoriju spadaju službenici prijemnih odjeljenja, službenici na telefonskoj centrali, sekretarice i pomoćnici te zaštitari.

UOBIČAJENE METE NAPADA

Uobičajene mete napada metodom socijalnog inženjeringa su žrtve koje nisu svjesne značaja informacija. U tu kategoriju spadaju službenici prijemnih odjeljenja, službenici na telefonskoj centrali, sekretarice i pomoćnici te zaštitari.

Mete napada mogu biti i osobe s posebnim ovlastima kao što su informatička i tehnička podrška korisnicima, administratori na informatičkim sustavima, računalni operateri i administratori na telefonskim sustavima.

Isto tako metodom socijalnog inženjeringa napadaju se i proizvođači i pružatelji usluga, a posebno proizvođači računalnog hardvera i softvera te proizvođači sustava za glasovnu poštu.

UOBIČAJENE METODE OBMANE

- Predstavlja se kao kolega.
- Predstavlja se kao djelatnik iz poduzeća koje je Vama dobavljač usluga, iz partnerskog poduzeća ili kao policijski službenik.
- Predstavlja se kao netko na višem položaju.
- Predstavlja se kao novi djelatnik kojem treba pomoć.
- Predstavlja se kao dobavljač usluga ili proizvođač računalnih sistema koji zove da bi ponudio sistemsku zakrpu ili najnoviju verziju.
- Nuđenje pomoći ako bi nastao problem, potom izazivanje problema, čime se žrtva navede da od napadača zatraži pomoć.
- Slanje besplatnih softvera ili zakrpa da ih žrtva instalira.
- Slanje virusa ili trojanskog konja u prilogu elektronske poruke.
- Upotreba lažnog okvira za dijalog u kojem se od žrtve traži da ponovno

podnese prijavu za rad ili ponovno unese lozinku.
- Snimanje žrtvinih pritisaka na tipkovnice pomoću računalnog sistema ili programa.
- Ostavljanje disketa ili kompakt diskova s zloćudnim softverom na radnom mjestu.
- Korištenje internom terminologijom da bi se zadobilo nečije povjerenje.
- Nuđenje nagrade da bi se netko registrirao na web lokaciju pomoću korisničkog imena i lozinke.
- Ostavljanje dokumenata ili datoteka u prostorijama za poštu neke kompanije radi isporuke u kancelarije.
- Prilagođavanja zaglavlja faxa tako da se čini da je poslan s interne lokacije.
- Zamolba službeniku prijemnog odjela da primi i proslijedi fax.
- Zahtjev da se datoteka proslijedi do naizgled interne lokacije.
- Podešavanje glasovne poruke tako da pozivatelji pomisle da im je napadač kolega.
- Pretvaranje napadača da dolazi iz drugog ogranka poduzeća i traženje da mu se u sistemu poduzeća otvori sandučić elektronske pošte.

ZNAKOVI KOJI UPOZORAVAJU NA MOGUĆI NAPAD

- Netko Vam odbija reći broj na koji ga možete dobiti.
- Neobičan zahtjev.
- Naglašavanje visokog položaja.
- Naglašavanje hitnosti slučaja.
- Prijetnja negativnim posljedicama u slučaju odbijanja suradnje.
- Spominjanje poznatih osoba.
- Nelagodno ispitivanje pri razgovoru.
- Dijeljenje komplimenata ili laskanje.
- Flert.

FAKTORI KOJI OLAKŠAVAJU NAPAD NA TVRTKE

- Veliki broj zaposlenih.
- Više ogranaka.
- Podaci o lokaciji zaposlenika u porukama glasovne pošte.
- Objavljivanje internog i skraćenog telefonskog broja.
- Nepostojanje sigurnosne obuke djelatnika na svim razinama.
- Nepostojanje sistema klasifikacije tajnosti podataka.
- Nepostojanje protokola za prijavu incidenata i reagiranja na njih.

Postoje ljudi koji cijeli dan leže potrbuške i razmišljaju kako da Vas „klepe“. To što Vi ne znate za njih ne znači da i ne postoje! General Security radi savjetovanja i izobrazbu Vaših djelatnika i Vas da lakše i na vrijeme prepoznate ove suptilne metode napada. General Security is what we do.