

Den menneskelige faktor anses af mange sikkerhedseksperter som værende ét af de svageste led i sikkerhedsforsvaret.

En organisation kan således have den perfekte tekniske sikring af dens IT-installationer og stadig være yderst sårbar over for angreb på det menneskelige niveau.

“Social engineering” er betegnelsen for angreb der netop retter sig imod menneskelige procedurer. Social engineering er en samling af teknikker som anvendes til at manipulere personer til at udføre uautoriserede handlinger eller til at afsløre fortrolige informationer. Ved social engineering udgiver angriberen sig for at være en person der er autoriseret til at få udført de ønskede handlinger. Samtidig opdigter angriberen et scenario som gør det sandsynligt at ofret vil efterkomme hans ønsker.

Sikkerhedstesten deles dermed overordnet op i to faser:

1. Informationsindsamling mht. hvilke personer som er autoriseret til at udføre de ønskede handlinger. Derudover indsamles informationer om disse personer eller om organisationen og dennes IT-installationer, der kan anvendes til at skabe et realistisk scenario.
2. Udførelse af selve social engineering-angrebet. Målet for sikkerhedsvurderingen udvælges blandt de indsamlede informationer og er en person eller afdeling som vurderes at have mulighed for at udføre de ønskede handlinger. Angrebet kan udføres pr. e-mail, telefon, brev, fax eller sågar ved at angriberen møder op personligt.

Målet for sikkerhedstesten er at undersøge hvorvidt personer kan bringes til at udføre uautoriserede handlinger, som krænker fortrolighed eller integritet for udvalgte IT-installationer. Ydelsen er dermed en auditering af de menneskelige procedurer og arbejdsgange der anvendes i organisationen.

Option: Fysisk overvågning

Ydelsen kan suppleres med overvågning af organisationens fysiske perimeter via specialudstyr. Bl.a. opserveres og analyseres personers ankomst til og afgang fra organisationen, den fysiske adgangskontrol og mulige frie synsvinkler hvorved fortrolig information kan opsnappes (“shoulder surfing”). Aflytninger kan ligeledes foretages. Informationerne fra den fysiske overvågning kan være endog meget værdifulde for en angriber, ikke mindst når kombineret med social engineering-angreb.

Option: Test af procedure for makulering

Den typiske organisation udskriver hver dag enorme mængder information på papir. En del af denne information er fortrolig. Det er derfor vigtigt at en korrekt procedure for makulering forefindes samt at denne procedure også efterleves i praksis. Sker dette ikke, risikerer man at insidere eller outsiders opnår kendskab til de fortrolige oplysninger. Denne type angreb omtales ofte i faglitteraturen som “trashing”.