SOCIALNI INŽENIRING

Ali vaši zaposleni vedo, kakšna so pravila varovanja informacij?

Organizaciji, ki ima opravka z večjim številom različnih profilov zaposlenih, predstavlja zagotavljanje ustreznega nivoja varovanja informacij velik izziv. Najučinkovitejši način preverjanja ozaveščenosti in izobraževanja zaposlenih je izvedba t. i. socialnega inženiringa.

Socialni inženiring je nabor tehnik, s katerimi napadalec prelisiči ali prepriča uporabnika, da izvede določeno aktivnost (npr. odpre zlonamerno elektronsko pošto, uporabi ključ USB, okužen s škodljivo kodo, itd.) in s tem napadalcu omogoči dostop do zaupnih podatkov organizacije. Pri tem napadalec izkoristi odziv uporabnika na določeno situacijo (npr. na vabljivo ponudbo, zaupanje, pripravljenost pomagati itd.).
Poznamo več oblik socialnega inženiringa:

- tehnične metode,
- osebni stik,
- grožnje in izsiljevanja.

Za izvedbo socialnega inženiringa je potrebno zbrati veliko informacij o organizaciji in potencialnih tarčah (zaposlenih). Informacije se lahko pridobivajo s pomočjo javno dostopnih informacij (internetne strani, telefonski imeniki itd.), obiskov organizacije ali navezovanja prijateljskih stikov z zaposlenimi.

Primeri scenarijev preverjanja zaposlenih:

- pošiljanje »zlonamernih« elektronskih sporočil,
- podtikanje škodljive kode na prenosnem mediju,
- namestitev »zlonamerne« aplikacije na mobilni napravi,
- priklop neavtorizirane naprave v interno omrežje organizacije,
- pridobivanje informacij preko telefona, osebno, po klasični ali elektronski pošti,
- vstop v poslovne prostore brez identifikacije pri vhodu,
- vstop v varovano območje z izdajanjem identitete drugega.

Na podlagi izvedenih scenarijev se pripravi poročilo s statistiko uspešnosti napadov ter predlogi za izboljšanje ozaveščenosti zaposlenih na področju varovanja informacij in za nadgradnjo obstoječih varnostnih mehanizmov.

Informacije
SIQ Ljubljana
Preverjanje informacijskih tehnologij
T: 01 4778 345
E: infosec@siq.si

www.siq.si