PREPOZNAVANJE IN ODZIVANJE NA INFOSEC NAPADE

Na tem izobraževanju se bomo poglobili v načine varovanja podjetja pred napadi in načine pravilnega odzivanja na napade znotraj pravnih okvirjev. Zanimala nas bo tudi komunikacija z nadrejenimi in prijavitelji napada, kot tudi svetovanje službi, ki skrbi za človeške vire, ter pravnim in PR službam. Izobraževanje je namenjeno tehničnemu osebju – sistemskim administratorjem, CISO, CTO, vodjem in članom skupin, ki se v podjetju odzivajo na incidente, torej CERT v generičnem smislu besede.

Namen:

- Kako prepoznati vektor napada in model grožnje na tehničnem nivoju?
- Izvedba preventivnih ukrepov.
- Poznavanje pooblastil, dolžnosti in odgovornosti, ki jih ima posameznik, ki skrbi za informacijsko varnost.
- Boljša seznanjenost s komunikacijskimi prvinami, ko poročamo o napadih svojim nadrejenim.
- Poznavanje postopkov, ki bodo z večjo verjetnostjo zagotovili, da nam bodo zaposleni še kdaj poročali o incidentih.
- Prepoznavanje etične odgovornosti o razkrivanju incidentov.

Vsebina:

- Osvežitev izrazoslovja.
- Varovanje podjetja pred napadom (OSINT, penetracijsko testiranje lastne infrastrukture, baze podatkov o vdorih, sodelovanje s CERTi, stalno posodabljanje znanja, posodabljanje strojne in programske opreme, razvoj varnostnih politik, primeri dobre prakse ...).
- Prepoznavanje incidentov (pregled netflow dnevnikov, etično sledenje napadu, uporaba namenskih spletnih strani, ki analizirajo napade ...).
- Odzivi na napade znotraj pravnih okvirjev - kako zaustaviti napadalce in pri tem ne končati v ječi, ker smo mi kršili zakonodajo?
- Komunikacija z nadrejenimi o incidentu in njegovih posledicah.
- Svetovanje pravnim in PR službam ter službi, ki skrbi za človeške vire.
- Komunikacija s prijaviteljem napada.
- Odgovorno razkrivanje napadov (i. e. Responsible disclosure).

Trajanje: 8 šolskih ur

Ključni izvajalci: as. dr. David Modic