INFORMACIJSKI POOBLAŠČENEC

ICS
Institut za korporativne varnostne študije

si·cert

Posvet o odgovornem razkrivanju varnostnih ranljivosti

Ljubljana, 9. maj 2017

Zakaj posvet?

Pojav večjega števila javno razkritih varnostnih ranljivosti

Pogrešamo široko in odprto javno razpravo o odgovornem razkrivanju in etičnem hekanju

Nevarnosti:
za hekerja: KD Zlorabe OP, Napada na informacijski sistem;
za upravljavca zbirk OP prekrška (slabo zavarovanje OP);
nepopravljiva škoda za posameznike, poslovne subjekte, upravljavce

Dogovor o nadaljnjih korakih s ciljem **opredelitve/definiranja** odgovornega razkrivanja za doseganje boljše informacijske varnosti

(Ne)odgovorno razkrivanje varnostnih ranljivosti

Razkritja ranljivosti informacijskih sistemov – ogroženi podatki
OP, TP, PS, davčne tajnosti, kritična infrastruktura države, ...

Vzroki za **nezadostno identifikacijo/upravljanje varnostnih groženj**?

Je (pravna) **definicija etičnega in neetičnega hekanja** možna?

Etični (dobronamerni) heker: (le) **najet ali** (tudi) **samoiniciativen** - je odgovoren za nastanek težav: škode, nedelovanje/izpad sistema, ….?

Koga obvestiti, kdaj in kako ob odkriti ranljivosti? Upravljavca/proizvajalca + Policijo, SI-CERT, AKOS, IP, pristojni nadzorni organ, javnost? + Rok za odpravo ranljivosti?

Smisel obveščanja: odprava napake ali panika/pozornost/izsiljevanje

Javno poročanje v zadnjih primerih odkritih varnostnih ranljivosti?
Ustrezno ali pretirano, pravočasno – prepozno – prezgodnje?

Obvestilo o kršitvi VOP po GDPR

a.) v primeru kršitev VOP (razen če ni verjetno, da bodo ogrožene TČP) mora **upravljavec v 72 urah obvestiti IP** (kršitev; kategorije in pribl. število posameznikov; katere zbirke OP; DPO; predvidene posledice kršitve; že sprejeti ukrepi).

b.) (le) če je verjetno, da kršitev VOP povzroči veliko tveganje za TČP, upravljavec brez nepotrebnega odlašanja kršitev obvesti **posameznika** (DPO, opis posledic in sprejetih ukrepov) – razen če: *je upravljavec že izvedel ustrezne tehnične in organizacijske zaščitne ukrepe glede kršitve ali *je že sprejel ukrepe za zagotovitev, da se veliko tveganje za TČP verjetno ne bo več udejanjilo ali * bi to zahtevalo nesorazmeren napor – v tem zadnjem primeru objavi javno sporočilo ali podoben ukrep, s katerim so posamezniki na katere se nanašajo OP, enako učinkovito obveščeni .

Kakšne zaključke pričakujemo od tega posveta?

- Nadaljevanje javnega diskurza

- Čimprejšnje koriščenje dobrih praks iz tujine

- Priprava predlogov za opredelitev odgovornega razkrivanja:

  - Koga, kdaj in kako se obvešča, kakšni so ustrezni roki, vloge in odgovornosti, postopki, poročanje?
  - Meje odgovornega razkrivanja, zaščita odgovornih prijaviteljev?
  - Kodeks odgovornega razkrivanja?
  - Vzorec izjave o obveščanju o varnostnih ranljivostih in zaščiti prijavitelja na spletnih straneh upravljavcev?
  - Kako prepričati državo, resorna ministrstva (MORS, MJU, MP), da je pojem odgovornega razkrivanja nujno čim bolj poenotiti in normirati?