Usklajeno razkrivanje ranljivosti in evropska podatkovna zbirka ranljivosti

Zakon o informacijski varnosti (ZInfV-1) v 17. členu določa koordinatorja za usklajeno razkrivanje ranljivosti v Republiki Sloveniji.

Ranljivost je pomanjkljivost, dovzetnost ali napaka proizvoda ali storitve informacijsko-komunikacijskih tehnologij (IKT), ki jo kibernetska grožnja lahko izkoristi.

Koordinator deluje kot zaupanja vreden posrednik in po potrebi olajšuje sodelovanje med fizično ali pravno osebo, ki poroča o ranljivostih, in proizvajalcem ali ponudnikom proizvodov ali storitev IKT, ki naj bi zajemali ranljivost na pobudo katere koli stranke.

V skladu s prehodno določbo 59. člena ZInfV-1 je koordinator za usklajeno razkrivanje ranljivosti v Republiki Sloveniji SI-CERT, ki deluje kot notranja organizacijska enota pri javnem infrastrukturnem zavodu Akademska in raziskovalna mreža Slovenije.

Fizične ali pravne osebe iz prvega odstavka tega člena lahko koordinatorju o ranljivostih poročajo anonimno. Koordinator zagotovi skrbno nadaljnje ukrepanje v zvezi s sporočenimi ranljivostmi in anonimnost fizične ali pravne osebe, ki je o ranljivosti poročala. Kadar bi lahko sporočena ranljivost pomembno vplivala na subjekte tudi v drugih državah članicah Evropske unije, koordinator po potrebi sodeluje z drugimi skupinami za odzivanje na incidente na področju računalniške varnosti (CSIRT), ki so kot koordinatorke imenovane v okviru mreže skupin CSIRT.

Agencija Evropske unije za kibernetsko varnost (ENISA) je vzpostavila evropsko podatkovno zbirko ranljivosti, s katero želi okrepiti digitalno varnost Evrope.