REPUBLIKA SLOVENIJA
URAD VLADE RS ZA INFORMACIJSKO VARNOST

Ulica gledališča BTC 2, 1000 Ljubljana

T: 01 478 4778
E: gp.uiv@gov.si
W: http://www.uiv.gov.si
Twitter: @URSIV_Slovenia

Številka: 386-42/2025-1544-6
Datum: 26. 11. 2025

Zadeva: Priporočila za izvajanje ukrepov za preprečitev dostopa do podatkovnih zbirk

Pristojni nacionalni organ za informacijsko varnost (v nadaljevanju URSIV) je upravljal s težjim incidentom stopnje C3, v okviru katerega je prišlo do nepooblaščenega dostopa do zbirk podatkov. URSIV ocenjuje, da nepooblaščen dostop do zbirk podatkov predstavlja varnostno tveganje informacijske in kibernetske varnosti tako za zavezance, kot tudi za fizične osebe.

URSIV na podlagi tretjega odstavka 37. člena Zakona o informacijski varnosti (ZInfV-1),[1] glede na trenutno oceno ogroženosti, izdaja priporočila za izvedbo dodatnih ukrepov za varnost omrežij ali informacijskih sistemov.

V primeru, da zbirke podatkov obsegajo tudi osebne podatke, se na podlagi 23. člena Zakona o varstvu osebnih podatkov (ZVOP-2)[2], za varnost osebnih podatkov na področju posebnih obdelav za določene informacijske sisteme[3] smiselno uporabljajo določbe o ukrepih za obvladovanje tveganj in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na bistvene subjekte, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

Posledično z namenom ustreznega obvladovanja potencialnih tveganj in preprečevanja nastajanja znatnih operativnih motenj pri opravljanju storitev ali finančne izgube za zavezance in fizične osebe, ki bi izhajala iz nepooblaščenega dostopov do zbirk podatkov, URSIV subjektom, ki imajo v upravljanju zbirke podatkov, priporoča izvedbo naslednjih ukrepov:

- identificiranje in popis informacijskih sistemov na katerih se nahajajo zbirke podatkov (tudi osebnih) in njihovih skrbnikov ter upravljavcev,
- zagotavljanje revizijskih sledi dostopov do zbirk podatkov,
- varnostno preverjanje vseh informacijskih sistemov in aplikacij s katerimi in na katerih se hranijo in obdelujejo podatki,
- določitev ustreznih kriterijev za zagotavljanje visokih standardov kibernetske varnosti v postopku razvoja aplikacij, ki se uporabljajo za dostopanje ali obdelovanje podatkov,
- uvedba zahteve predhodnega varnostnega preverjanja aplikacij pri organizacijah, ki imajo zakonsko podlago za dostop do centraliziranih zbirk podatkov,
- uvedbo ali nadgradnjo sistema za zaznavanje in beleženje anomalij pri dostopih do zbirk podatkov,

[1] Uradni list RS, št. 40/25.
[2] Uradni list RS, št. 163/22 in 40/25 – ZInfV-1.
[3] 1. odstavek 23. člena ZVOP-2: (1) Za informacijske sisteme, v katerih:
1.se izvajajo obdelave osebnih podatkov, določenih v zakonih, ki urejajo področja upravnih notranjih zadev, finančne uprave, državljanstva, Slovenske obveščevalno-varnostne agencije, obrambe, zdravstvenega varstva, obveznega zdravstvenega zavarovanja, uveljavljanja pravic iz javnih sredstev ter kazenskih in prekrškovnih evidenc, ali
2. se obdelujejo osebni podatki več kot 100.000 posameznikov na podlagi zakona, razen obdelav osebnih podatkov iz 3. poglavja 2. dela tega zakona, ali
3.upravljavec ali obdelovalec kot svojo temeljno dejavnost izvaja obsežne obdelave posebnih vrst osebnih podatkov, ali
4.se obdeluje posebne vrste osebnih podatkov več kot 10.000 posameznikov.

- zapisi, pridobljeni z vpogledi v centralizirane zbirke podatkov se ne uporabljajo za vzpostavitev lastnih oziroma lokalnih zbirk podatkov,
- Izvedba analize tveganja delovnih procesov pri katerih se izvajajo dostopi ali obdelujejo podatki ter priprava preventivnih ukrepov za zamejitev tveganj,
- Izvedba analize tveganja obstoječih digitalnih platform, ki kot identifikator uporabljajo osebne podatke ter priprava preventivnih ukrepov za zamejitev tveganj,
- uporabo večfaktorske avtentikacije ali rešitev neprekinjene avtentikacije, kadar je to potrebno zaradi obvladovanja tveganj,
- spremljanje varnostnih obvestil pristojne skupine CSIRT ali pristojnega nacionalnega organa,
- politike in postopke v zvezi z uporabo oblačnih storitev, ki jih uporabljajo za svoje delovanje ali opravljanje storitev,
- osnovne prakse kibernetske higiene in usposabljanje na področju informacijske in kibernetske varnosti,
- izdelava načrta za odzivanje na kibernetske incidente in redno preverjanje postopkov odzivanja prek izvedbe simulacij kibernetskih incidentov, s katerimi se preveri odzivnost, pretok informacij in operativna pripravljenost.

S spoštovanjem,

Dr. Uroš Svete
Direktor urada