REPUBLIKA SLOVENIJA
MINISTRSTVO ZA DIGITALNO PREOBRAZBO
Davčna ulica 1, 1000 Ljubljana

T: 01 555 58 00
E: gp.mdp@gov.si
www.mdp.gov.si

MINISTRSTVO ZA DIGITALNO PREOBRAZBO
Davčna ulica 1
1000 Ljubljana

Številka: 382-209/2023-3150-9
Datum: 19. 04. 2024

Zadeva: Minimalne varnostne zahteve iz petega odstavka 8. člena Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov

Ministrstvo za digitalno preobrazbo na podlagi petega odstavka 8. člena Uredbe o varnostni dokumentaciji in minimalnih varnostnih ukrepih povezanih subjektov (Uradni list RS, št. 118/23) in drugega odstavka 18.a člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23) izdaja minimalne varnostne zahteve upravljavca centralnega informacijsko-komunikacijskega sistema (v nadaljevanju CIKS).

Informacijski sistem mora izpolnjevati minimalne varnostne zahteve, kar pomeni;

1. da mora imeti nameščeno programsko opremo zadnje (stabilne) verzije oziroma verzije, za katero se zagotavlja podpora proizvajalca programske opreme vključno z varnostnimi popravki, za katere je popravek proizvajalca na voljo in obstajajo znana orodja ali metode za zlorabo ranljivosti;
2. da mora imeti na vseh strežnikih in vseh delovnih postajah nameščeno programsko opremo za zašito končnih točk (EDR), ki se samodejno posodablja;
3. da hkrati poleg dostopa do CIKS nima drugih povezav do medmrežja (ne velja za uporabnike VPN povezav);
4. da za oddaljeno delo uporablja opremo pod upravljanjem in nadzorom skrbnika opreme povezanega subjekta in pri tem vedno vzpostavi VPN povezavo odobreno oziroma upravljano s strani upravljavca CIKS (velja tudi za uporabo oblačnih storitev);
5. da preprečuje fizični dostop do opreme informacijsko-komunikacijskega sistema (v nadaljevanju IKS) v upravljanju povezanega subjekta in upravljavca CIKS;
6. ne posega v opremo upravljavca CIKS;
7. da upravlja s pooblastili do dostopa uporabnikov do svojega IKS na način, da zagotavlja in upravlja dostope tistim svojim uporabnikom glede na potrebe delovnih nalog:
8. da za dostop do sistemov uporablja močna gesla oziroma več faktorsko avtentikacijo (MFA);
9. da neaktivne / neuporabljene mrežne priključke onemoči na logičnem nivoju oziroma po možnosti vpelje tehnologijo po standardu 802.1X;
10. da gostom ne dovoljuje nenadzorovano uporabo IKS subjekta (npr. dostop do interneta preko WIFI omrežij za goste preko CIKS);
11. da svoje uporabnike ozavesti o primerni rabi IKS in redno usposablja s področja informacijske varnosti.

Poleg zgornjih ukrepov Ministrstvo apelira povezane subjekte:

- k izvedbi varnostnih pregledov IKS povezanih subjektov,
- k posodobitvam programske opreme ter odpravi ranljivosti v svojih IKS,
- da na svojih spletnih straneh med kontakti objavi tudi kontakt osebe odgovorne za področje informacijske varnosti,
- k prijavi incidentov informacijske varnosti.

Ministrstvo bo kot upravljavec CIKS s skeniranji in nadzornimi sistemi redno preverjalo izpolnjevanje minimalnih zahtev povezanih subjektov in jih opozarjal o morebitnih odstopanjih, v primeru hujših groženj ali kršitev varnostne politike ministrstva pa lahko začasno preventivno ali zaradi zamejitve incidenta informacijske varnosti tudi odklopil od centralnega informacijsko-komunikacijskega sistema do bodisi odprave kršitve ali groženje. Odpravo upravljavec centralnega informacijsko-komunikacijskega sistema predhodno preveri.

Upravljavec CIKS bo do 1. 5. 2024 izvedel dodatne ukrepe s katerimi bo okrepil varnost CIKS. Med temi ukrepi bo tudi striktno preverjanje izpolnjevanja zahtev pri povezovanju v CIKS preko VPN povezav. Zato vse povezane subjekte pozivamo, da izvedejo vse zahteve iz točk 1, 2 in 4, kajti zaradi neustrezno izvedenih zahtev prijava v omrežje ne bo mogoča.

Pripravil:

mag. Damijan Marinšek, sekretar

dr. Emilija Stojmenova Duh
Ministrica