Smjernice za korelacijski pregled mjera kibernetičke sigurnosti


NCSC
HR

Obaveza definirana člankom 49. Uredbe o kibernetičkoj sigurnosti (u daljnjem tekstu: Uredba)

(1) Korelacijski pregled mjera iz Priloga II. Uredbe (u daljnjem tekstu: Korelacijski pregled), kao i svih podskupova ovih mjera, mapira iste na najvažnije europske i međunarodne norme i najbolje prakse iz otvorenih izvora. Cilj korelacijskog pregleda je olakšati provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima.

(2) Korelacijski pregled mapira podskupove mjera iz Priloga II. Uredbe na europske i međunarodne norme i najbolje prakse iz otvorenih izvora. Međunarodne norme koje koristi korelacijski pregled su: ISO/IEC 27001:2022, ISO/IEC 27002:2022, ISO/IEC 22301:2019, NIST CSF 2.0, NIST SP 800-53 i CIS v8, raspoložive preko tražilice. Također, koristi se i Katalog kontrola kojeg je donio Zavod za sigurnost informacijskih sustava (ZSIS) u sklopu Smjernica za provedbu samoprocjene kibernetičke sigurnosti, objavljene na službenoj mrežnoj stranici ZSIS-a (www.zsis.hr). U idućih nekoliko crtica pobliže se opisuju međunarodne norme koje su korištene u okviru korelacijskog pregleda.

- **ISO/IEC 27001:2022**: međunarodni standard koji opisuje okvir za sustav upravljanja informacijskom sigurnošću. Propisuje načine na koje organizirati informacijsku sigurnost u bilo kojoj vrsti organizacije. Temeljna norma za upravljanje informacijskom sigurnošću pomaže organizacijama u zaštiti svojih važnih informacija od zloupotrebe, oštećenja ili gubitka.

- **ISO/IEC 27002:2022**: međunarodni standard koji pruža smjernice za primjenu sigurnosnih kontrola navedenih u ISO/IEC 27001. Verzija iz 2022. godine donosi moderniziranu i reorganiziranu strukturu sigurnosnih kontrola, koje su sada grupirane u četiri tematske cjeline: organizacijske, fizičke, tehnološke i kontrole ljudi. Cilj standarda je pomoći organizacijama u odabiru i implementaciji odgovarajućih mjera za zaštitu informacija, u skladu s procjenom rizika i poslovnim zahtjevima.

- **ISO/IEC 22301:2019**: međunarodni standard koji definira zahtjeve za sustav upravljanja kontinuitetom poslovanja. Namijenjen je za korištenje u okviru sustava upravljanja organizacijom, kako bi osigurao da su aktivnosti vezane za kontinuitet poslovanja u skladu s općim ciljevima organizacije i da su učinkovite u smislu zaštite od prekida poslovanja. Ovaj standard pomaže organizacijama u identificiranju rizika i njihovom upravljanju, uspostavi plana kontinuiteta poslovanja, sprječavanju i smanjivanju utjecaja incidenta te ubrzavanju oporavka.

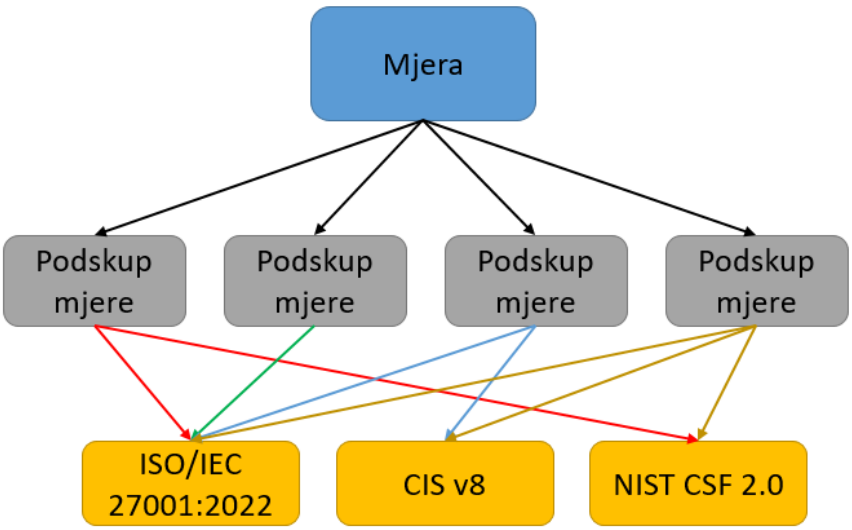
- **NIST CSF 2.0**: najnovija verzija američkog okvira za kibernetičku sigurnost koju je razvio *National Institute of Standards and Technology* (NIST). Ova verzija uključuje šest osnovnih funkcija: *Identify, Protect, Detect, Respond, Recover* i nova funkcija *Govern*, koja naglašava upravljanje sigurnosnim rizicima na strateškoj razini.

- **NIST SP 800-53**: dokument koji je objavio NIST, a pruža smjernice za implementaciju sigurnosnih kontrola u informacijskim sustavima američke savezne vlade. Standard sadrži opsežan skup kontrola koji se primjenjuju na različite aspekte sigurnosti, uključujući fizičku zaštitu, upravljanje pristupom, kriptiranje, upravljanje incidentima i mnoge druge.

- **CIS v8**: skup sigurnosnih kontrola koji pruža praktične smjernice za organizacije kako bi zaštitile svoje informatičke sustave i podatke od kibernetičkih prijetnji. CIS v8 također uzima u obzir nove tehnologije, poput računalstva u oblaku i mobilnih uređaja te pruža ažurirane preporuke za suočavanje s novim prijetnjama u današnjem digitalnom okruženju.

- **Katalog kontrola**: sadrži kontrole za mjere i podskupove mjera upravljanja kibernetičkim sigurnosnim rizicima propisanih Prilogom II. Uredbe. Kontrolom se smatra organizirani skup politika, procedura, procesa ili tehničkih mehanizama koji imaju za cilj upravljanje i smanjenje rizika u području kibernetičke sigurnosti kroz prevenciju, detekciju ili odgovor na potencijalne prijetnje.

(3) Korelacijski pregled, za svaki pojedini podskup mjere, navodi primjere kontrola iz navedenih međunarodnih normi i ZSIS-ovog Kataloga kontrola koje su tematski srodne te funkcionalno povezane. Nadalje, opseg svake pojedine kontrole navedenih međunarodnih normi i Kataloga kontrola nadilazi opseg podskupa mjere za kojeg se provodi mapiranje. Potrebno je naglasiti kako podskup mjere definira zahtjeve za obveznike ZKS-a, a kontrole iz korelacije pri tome se mogu koristiti za rješavanje zahtjeva ZKS-a. Cijela tablica s mapiranim kontrolama je u svojstvu priloga ovom dokumentu. Na Slici 1. je prikazana hijerarhija mjere, podskupa mjere i kontrole iz međunarodne norme koja pobliže prikazuje proces mapiranja pojedinog podskupa mjere na međunarodne norme.



Slika 1. Hijerarhija procesa mapiranja na međunarodne norme

(4) Korelacijski pregled donosi središnje državno tijelo za kibernetičku sigurnost.

Sigurnosno-obavještajna agencija

Nacionalni centar za kibernetičku sigurnost

Savska cesta 39/1, 10000 Zagreb

Republika Hrvatska

KONTAKT:

E-mail: info@ncsc.hr

www.ncsc.hr