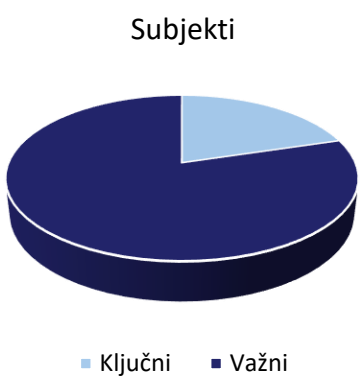
Pregled implementacije ZKS-a

Q2 2026

Zakonom o kibernetičkoj sigurnosti (ZKS) i njegovim podzakonskim aktima uređeno je područje kibernetičke sigurnosti u Republici Hrvatskoj, a za njegovu provedbu je početkom 2025. godine u SOA-i osnovan Nacionalni centar za kibernetičku sigurnost (NCSC-HR).
NCSC-HR, osim državno-sponzoriranih kibernetičkih APT napada, prati i kibernetičke napade na ključne i važne subjekte obveznike ZKS-a te na javni sektor.

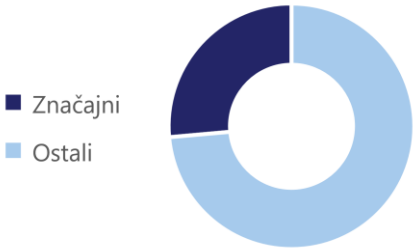


Nastavljen je proces utvrđivanja obveznika ZKS-a te je s krajem drugog kvartala 2026. godine u Republici Hrvatskoj kategorizirano 798 pravnih osoba obveznika ZKS-a, od kojih je 162 ključnih subjekata i 636 važnih subjekata.

U svrhu prevencije kibernetičkih napada i njihovih posljedica, NCSC-HR je kategoriziranim subjektima dostavio dodatne preporuke o provedbi zakonom utvrđenih mjera kibernetičke sigurnosti, kao i upitnik u svrhu procjene trenutnog stanja provedbe mjera.

Vlada Republike Hrvatske je na 185. sjednici održanoj 16. srpnja 2026. godine donijela Uredbu o provedbi Akta o kibernetičkoj solidarnosti (*Cyber Solidarity Act*), punog naziva Uredba (EU) 2025/38 Europskog parlamenta i Vijeća od 19. prosinca 2024. o utvrđivanju mjera za povećanje solidarnosti i kapaciteta u Uniji za otkrivanje kibernetičkih prijetnji i incidenata, pripremu za njih i odgovor na njih te o izmjeni Uredbe (EU) 2021/694 (Akt o kibernetičkoj solidarnosti).

Akt o kibernetičkoj solidarnosti usmjeren je na izgradnju sposobnosti Europske unije za odgovor na kibernetičke incidente. Akt uspostavlja europski sustav uzbunjivanja u području kibernetičke sigurnosti kroz mrežu nacionalnih i prekograničnih kibernetičkih centara država članica, mehanizam za izvanredne kibernetičke sigurnosne situacije kroz koordinirano testiranje pripravnosti i pričuvu Europske unije za kibernetičku sigurnost te europski mehanizam za istraživanje kibernetičkih sigurnosnih incidenata.



Subjekti obveznici ZKS-a su u drugom kvartalu 2026. godine prijavili ukupno 87 kibernetičkih incidenata, od kojih je 23 značajnih te 64 ostalih kibernetičkih incidenata. Prijavljeni kibernetički incidenti primarno su obuhvatili javni sektor, a uzroci incidenata uglavnom su bili ispadi usluge zbog tehničkih kvarova, iskorištavanje ranjivosti web aplikacija te *phishing* napadi.

Među prijavama značajnih incidenata, ističu se dva ucjenjivačka (*ransomware*) kibernetička napada. Kod ovakvih napada, napadači najčešće iskorištavaju poznate ranjivosti javno izloženih servisa ili kompromitirane lozinke VPN računa bez dvofaktorske autentifikacije.

Sustav SK@UT, nacionalni sustav za otkrivanje kibernetičkih prijetnji, štiti više od 120 državnih tijela, operatora kritične infrastrukture i pravnih osoba od posebnog interesa za Republiku Hrvatsku. Sustavom SK@UT je u 2026. godini zabilježen značajan porast broja državno-sponzoriranih kibernetičkih napada prema ciljevima u Republici Hrvatskoj.

Trend velikog porasta broja kibernetičkih napada u 2026. godini ukazuje na nužnost striktne provedbe mjera kibernetičke sigurnosti utvrđenih Zakonom o kibernetičkoj sigurnosti, što će značajno pridonijeti podizanju kibernetičke otpornosti Republike Hrvatske.

Provedba osnovne razine mjera kibernetičke sigurnosti može spriječiti ili znatno umanjiti učinak najvećeg broja napada, koji rezultiraju krađom osobnih ili osjetljivih podataka te zaustavljanjem poslovnih procesa.

Manji broj zabilježenih kibernetičkih napada je bio više razine sofisticiranosti, dok je većina ostalih napada bila oportunističke prirode i koristila je pogreške i propuste u konfiguraciji i održavanju mrežnih i informacijskih sustava.

Napominjemo, gotovo svi oportunistički kibernetički napadi ne bi bili uspješni da su bile provedene osnovne mjere kibernetičke sigurnosti.

NCSC HR