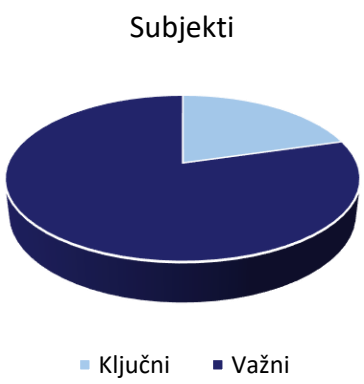
Pregled implementacije ZKS-a

Q1 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 u prvom kvartalu 2026. godine dodatno provedena kategorizacija subjekata iz sektora Upravljanja uslugama IKT-a (B2B).

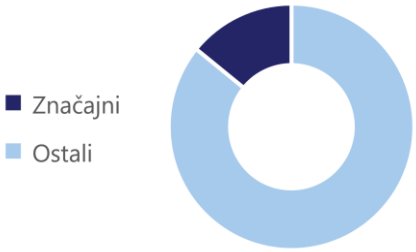
U Republici Hrvatskoj je do sada kategorizirano **790** pravnih osoba obveznika ZKS-a, koje su započele usklađenu provedbu mjera kibernetičke sigurnosti i prijavu kibernetičkih incidenata. Od toga su **162** ključna subjekta, a **628** važnih subjekata.

Većini obveznika ZKS-a u travnju 2026. godine istječe godina dana prilagodbe za uspostavu propisanih mjera kibernetičke zaštite. Kako bi pomogao u prilagodbi, NCSC-HR za subjekte iz svoje nadležnosti održava konzultacije o provedbi ZKS-a, a na mrežnoj stranici kontinuirano objavljuje odgovore na najčešća *Pitanja kategoriziranih subjekata*.

Daljnji razvoj zakonodavnog okvira u 2026. godini temelji se na donošenju Uredbe o provedbi EU Akta o kibernetičkoj solidarnosti te izradi novog nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti.

Akt o kibernetičkoj solidarnosti 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.

NCSC HR



Subjekti obveznici ZKS-a su u prvom kvartalu 2026. godine prijavili ukupno **106** kibernetičkih incidenata, od kojih je **15** značajnih te 91 ostali kibernetički incident. Većina prijavljenih značajnih incidenata se odnosila na ispade usluga čiji je uzrok tehnički kvar, a ostali prijavljeni incidenti većinom su *phishing* napadi i druge prijevare.

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, kao nacionalni sustav za otkrivanje kibernetičkih prijetnji, štiti više od 110 državnih tijela, operatora kritične infrastrukture i pravnih osoba od posebnog interesa za Republiku Hrvatsku. U prvom kvartalu 2026. godine, sustavom SK@UT zabilježen je značajan porast broja državno-sponzoriranih kibernetičkih napada na ciljeve u Republici Hrvatskoj u odnosu na prethodne kvartale.

Sve veća prijetnja postaju kibernetički napadi putem lanca opskrbe (*supply chain attack*) u kojima se kompromitacijom dobavljača pokušava ostvariti krajnji cilj napada. Napadači tako lakše prikrivaju svoje djelovanje te im se otvara mogućnost napada na cijeli niz potencijalnih ciljeva. Ovakvi napadi ukazuju kako je posebnu pažnju u provedbi politika kibernetičke sigurnosti potrebno usmjeriti na sigurnost lanca opskrbe, osobito na upravljanje uslugama IKT-a.

Uz kontinuiranu prijetnju koju predstavljaju ucjenjivački (*ransomware*) kibernetički napadi na kritične sektore, u ovom kvartalu zamijećen je porast broja državno-sponzoriranih kibernetičkih napada, a sve veća prijetnja postaju i napadi putem lanca opskrbe. Analiza aktualnih kibernetičkih napada ukazuje da se provedbom osnovne razine mjera kibernetičke zaštite može spriječiti ili znatno umanjiti učinak najvećeg broja napada.

NCSC HR