



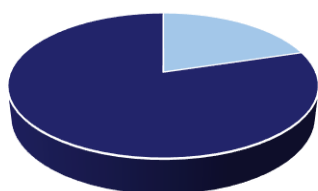
Pregled implementacije ZKS-a

Q3 2026

Zakonom o kibernetičkoj sigurnosti (ZKS) i njegovim podzakonskim aktima uređeno je područje kibernetičke sigurnosti u Republici Hrvatskoj.

Nacionalni centar za kibernetičku sigurnost (NCSC-HR) ustrojen je u okviru Sigurnosno-obavještajne agencije s ciljem zaštite nacionalnog kibernetičkog prostora te obavljanja zadaća središnjeg državnog tijela za kibernetičku sigurnost, nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti, CSIRT-a, tijela odgovornog za upravljanje kibernetičkim krizama i jedinstvene kontaktne točke prema ZKS-u.

Subjekti



■ Ključni ■ Važni

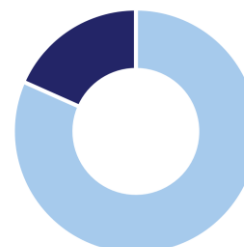
Nastavljen je proces utvrđivanja obveznika ZKS-a te je trenutno u Republici Hrvatskoj kategorizirano 799 pravnih osoba, od kojih su 162 ključna subjekta i 637 važnih subjekata.

Subjekti obveznici ZKS-a su u trećem kvartalu 2026. godine prijavili ukupno 125 kibernetičkih incidenata, od kojih je 23 značajnih te 102 ostala kibernetička incidenta.

Većina prijavljenih kibernetičkih incidenata se odnosila na ispađe usluga čiji je uzrok tehnički kvar, *phishing* napade i druge oblike prijevara.

Ucjenjivački (*ransomware*) kibernetički napadi i dalje predstavljaju ozbiljnu prijetnju. U trećem kvartalu zabilježeno je sedam ovakvih napada, od kojih je šest spriječeno prije zaključavanja infrastrukture od strane napadača.

■ Značajni
■ Ostali



Početkom listopada u Zagrebu je u organizaciji NCSC-HR održana Četvrta SK@UT konferencija na kojoj je sudjelovalo gotovo 450 sudionika.

Na konferenciji je naglašena potreba za sustavnim jačanjem kibernetičke otpornosti organizacija. Cilj je graditi organizacije koje mogu prepoznati i spriječiti prijetnje, ali i brzo reagirati, zaštititi ključne procese, oporaviti se te nastaviti funkcionirati i nakon kibernetičkog napada.



U tijeku je izrada Nacionalnog plana kibernetičke sigurnosti od 2027. do 2031. godine te prijedloga Zakona o provedbi EU Akta o kibernetičkoj otpornosti (*Cyber Resilience Act*).

EU Aktom o kibernetičkoj otpornosti povećat će se razina kibernetičke sigurnosti proizvoda s digitalnim elementima na EU tržištu uvođenjem obveznih sigurnosnih zahtjeva tijekom njihova životnog ciklusa.

U rujnu je u rad puštena EU Jedinstvena platforma za izvješćivanje (*Single Reporting Platform*) koja proizvođačima proizvoda s digitalnim elementima omogućuje ispunjavanje obveza prijavljivanja aktivno iskorištenih ranjivosti i incidenata koji imaju značajan utjecaj na sigurnost proizvoda.

Analizom niza naprednih kibernetičkih napada na ciljeve u Republici Hrvatskoj u 2026. godini, potvrđeno je kako napadači u sve većoj mjeri koriste alate umjetne inteligencije. Navedeni alati su korišteni kako bi značajno ubrzali proces otkrivanja i iskorištavanja ranjivosti, posebice u namjenski izrađenim web aplikacijama koje nisu prošle adekvatno sigurnosno testiranje. U napadima su korišteni komercijalni modeli umjetne inteligencije, a napadači su iskorištavali tehnike zaobilazanja ugrađenih sigurnosnih mehanizama (*jailbreak*), kako bi ih mogli koristiti za provođenje napada.

Naglašavamo važnost provedbe svih propisanih mjera kibernetičke sigurnosti, a po pitanju ove prijetnje posebice ističemo obaveznu dvofaktorsku autentifikaciju te provođenje sigurnosnih testiranja namjenski izrađenih web aplikacija.

Trend velikog porasta broja kibernetičkih napada u 2026. godini ukazuje na nužnost striktno provedbe mjera kibernetičke sigurnosti utvrđenih ZKS-om. Navedeno 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.