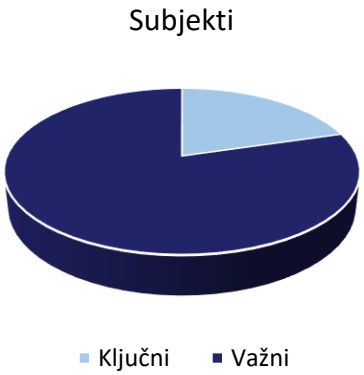
Pregled implementacije ZKS-a

Q4 2025

Zakonom o kibernetičkoj sigurnosti (ZKS) i njegovim podzakonskim aktima uređeno je područje kibernetičke sigurnosti u Republici Hrvatskoj (RH), a za njegovu provedbu je početkom 2025. godine u SOA-i osnovan Nacionalni centar za kibernetičku sigurnost (NCSC-HR).

NCSC-HR se, osim praćenja državno-sponzoriranih kibernetičkih APT napada, bavi i praćenjem značajnih kibernetičkih napada na ključne i važne subjekte prema ZKS-u, kao i ostalim kibernetičkim incidentima.



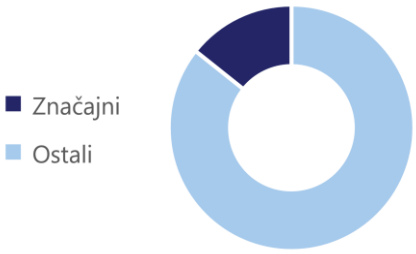
Nastavljen je proces utvrđivanja obveznika ZKS-a te su, među ostalima, kategorizirani i informacijski posrednici u okviru Fiskalizacije 2.0.

Do ovog trenutka u Republici Hrvatskoj je kategorizirano 780 pravnih osoba obveznika zakona, koje su započele usklađenu provedbu mjera kibernetičke sigurnosti i prijavu kibernetičkih incidenata. Od toga je 159 ključnih i 621 važan subjekt.

NCSC-HR je u listopadu 2025. godine pozvao sve pravne osobe koje posluju u RH, a ne zadovoljavaju kriterije za kategorizaciju, da se dobrovoljno uključe u provedbu mjera kibernetičke sigurnosti. Za sve pravne osobe koje ne žele pristupiti opisanom okviru za dobrovoljnu provedbu mjera preporučuje se samostalno provođenje minimalnih mjera za jačanje kibernetičke otpornosti koje su opisane na mrežnim stranicama NCSC-HR u rubrici *Dokumenti/Preporuke*.

Daljnji razvoj zakonodavnog okvira provodi se kroz pripremu novog nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti, za što je osnovana međuresorna radna skupina.

NCSC-HR je započeo redovne stručne konzultacije o provedbi ZKS-a s kategoriziranim subjektima. Odgovori na najčešća pitanja subjekata dostupni su na mrežnim stranicama NCSC-HR u rubrici *Česta pitanja/Pitanja kategoriziranih subjekata*.



Subjekti obveznici ZKS-a su u četvrtom kvartalu 2025. godine prijavili ukupno 91 kibernetički incident, od kojih je 13 značajnih te 78 ostalih kibernetičkih incidenata.

Među značajnim incidentima, ističu se dva ucjenjivačka (*ransomware*) napada iza kojih stoje financijski motivirane kibernetičke kriminalne grupe. Također, prijavljeno je i nekoliko slučajeva ucjenjivačkih (*ransomware*) napada na pravne osobe koje nisu obveznici ZKS-a. Kao trenutno najaktivnija u svijetu i u RH, ističe se kriminalna grupa Qilin.

Od ostalih značajnih kibernetičkih incidenata treba napomenuti kako se u slučaju jednog napada na kritičnu infrastrukturu, u procesu odgovora na incident, koristio EU mehanizam *Cybersecurity Reserve* te je RH postala prvom državom članicom koja je koristila navedeni mehanizam.

U listopadu 2025. godine održana je Treća SK@UT konferencija. SK@UT konferencija predstavlja jednu od najvećih nacionalnih konferencija o kibernetičkoj sigurnosti, a ove godine okupila je više od 350 sudionika predstavnika SK@UT zajednice.

Dana 18. prosinca 2025. godine WatchGuard je objavio informacije o ranjivosti kritične razine (CVE-2025-14733) u WatchGuard Firebox vatrozidima. NCSC-HR je sigurnosno upozorenje vezano za ovu ranjivost objavio na svojim mrežnim stranicama i na komunikacijskom kanalu SK@UT zajednice te su i izravno upozorene organizacije za koje je NCSC-HR utvrdio kako koriste potencijalno ranjive WatchGuard vatrozide.

Najveću kratkoročnu prijetnju i dalje predstavljaju ucjenjivački (*ransomware*) napadi na državni sektor i druge kritične sektore. Provedbom ZKS mjera, koje su određene temeljem procjene veličine i sektora subjekata, kategorizirani subjekti postat će otporniji na sve vrste kibernetičkih napada. Provedba mjera je postupna te će se povećanje otpornosti subjekata na kibernetičke napade moći jasnije vidjeti u narednom razdoblju.