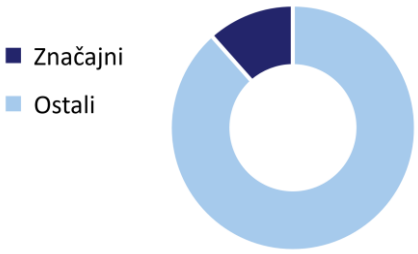
# Pregled implementacije ZKS-a

Q3 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). Republika Hrvatska je po prvi puta dobila središnje državno tijelo za kibernetičku sigurnost.
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.


Jedan od najznačajnijih koraka u implementaciji ZKS-a je kontinuirano provođenje kategorizacije obveznika zakona. Sva nadležna tijela su usklađeno i koordinirano provela inicijalnu kategorizaciju u travnju 2025. godine, nakon čega je ovaj proces nastavljen sukladno specifičnostima pojedinih sektora. Do sad je kategorizirano 713 pravnih osoba obveznika zakona koje su započele usklađenu provedbu mjera kibernetičke sigurnosti i prijavu kibernetičkih incidenata. Od toga je 125 ključnih i 588 važnih subjekata.

Nastavlja se nacionalno zakonodavno uređenje područja kibernetičke sigurnosti. Vlada RH je 26. rujna 2025. godine usvojila Plan provedbe vježbi kibernetičke sigurnosti za razdoblje do 2027. godine, što je prvi nacionalni dokument ove vrste u području kibernetičke sigurnosti. Time se uvodi cjelovit i sustavan pristup planiranju provedbi vježbi kibernetičke sigurnosti na nacionalnoj razini.




Subjekti obveznici ZKS-a su u trećem kvartalu 2025. godine prijavili ukupno 104 kibernetička incidenta, od kojih je 12 značajnih te 92 ostala kibernetička incidenta.

Među značajnim incidentima, u dvije trećine slučajeva se radilo o ispadima usluga koji su zadovoljili kriterije za značajni incident, a uz njih se ističu i dva incidenta vezana uz kompromitacije Microsoft SharePoint Servera. Od ostalih prijavljenih kibernetičkih incidenata, većina su bili *phishing* napadi te druge vrste neželjenih poruka.

Sustav SK@UT, kao nacionalni sustav za otkrivanje kibernetičkih prijetnji, proširen je na ukupno više od 100 državnih tijela, operatora kritične infrastrukture i pravnih osoba od posebnog interesa za RH. Tijekom 2025. godine prioritet uključenja u sustav su bolničke ustanove i institucije iz sektora zdravstva.

Microsoft je 19. srpnja 2025. godine objavio informacije o kritičnoj ranjivosti Microsoft SharePoint Servera koje su napadači aktivno iskorištavali. NCSC-HR je na svojim mrežnim stranicama objavio sigurnosno upozorenje te dodatno obavijestio subjekte iz svoje nadležnosti na čijoj je infrastrukturi zamijećen javno dostupni SharePoint servis. U jednom od prijavljenih značajnih incidenata iz trećeg kvartala 2025. godine, iskorištavanje ove ranjivosti bio je inicijalni vektor ucjenjivačkog (*ransomware*) napada.

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 otpornost subjekata na kibernetičke napade moći jasnije vidjeti u bliskoročnom razdoblju.

NCSC HR