CARNET

CERT.hr GODIŠNJI IZVJEŠTAJ 2025

Sadržaj

Uvod

Tijekom 2025. godine Nacionalni CERT je provodio svoje proaktivne i reaktivne mjere, projekte, održao edukacijske i druge aktivnosti posvećene podizanju svijesti o kibernetičkoj sigurnosti, informirao korisnike o kibernetičkim prijetnjama, ranjivostima i incidentima kroz medijska pojavljivanja i objave upozorenja putem društvenih mreža i web sjedišta te je redovito provjeravao sustave u svojoj nadležnosti te informirao korisnike o pronađenim ranjivostima i mjerama koje je potrebno provesti u svrhu očuvanja sigurnosti kibernetičkog prostora RH i zaštite građana.

Statistički podaci pokazuju značajan porast u broju obrađenih incidenata u 2025. godini u odnosu na 2024. godinu. Obrađeno je 1513 incidenata, pri čemu je važno naglasiti da se ovaj broj odnosi samo na incidente za koje je Nacionalni CERT zaprimio prijavu ili ih otkrio vlastitim aktivnostima. Vodeći tipovi incidenata su: phishing napad (32 %), neželjene poruke (19 %), ostale vrste financijski motiviranih prijevara (18 %), napadačka infrastruktura (12 %).

Zbroj zabilježenih botova prema tipu (vrsti zlonamjernog sadržaja) tijekom 2025. godine iznosi 126 098, što je smanjenje od 33,37 % u odnosu na 2024. godinu.

Nacionalni CERT nastavio je s razvojem PiXi platforme, putem koje je od svibnja 2025. godine omogućeno ispunjavanje obveza prijave incidenata kategoriziranim subjektima temeljem Zakona o kibernetičkoj sigurnosti (NN 14/24).

Bilježimo povećanje korištenja usluga CERT iffy sustava, namijenjenog za provjeru internetskih trgovina. Tijekom 2025. godine provjeren je 37 191 URL.

Nacionalni CERT surađuje s brojnim institucijama i organizacijama na nacionalnoj, europskoj i međunarodnoj razini kao što su drugi CERT timovi, institucije EU-a i NATO-a u svrhu postizanja zajedničkih ciljeva u području kibernetičke sigurnosti.

U svrhu razvoja kompetencija, podizanja spremnosti i svijesti o kibernetičkoj sigurnosti Nacionalni CERT je aktivno sudjelovao u NATO vježbi „Cyber Coalition 2025“, u kojoj su testirane tehničke, operativne i pravne procedure kao i spremnost na krizno komuniciranje.

CARNET-ov Nacionalni CERT aktivno sudjeluje u obilježavanju Europskog mjeseca kibernetičke sigurnosti provedbom niza aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti. Provedeno je šesto nacionalno CTF natjecanje iz područja kibernetičke sigurnosti za srednjoškolce Hacknite i drugo CTF natjecanje za studente – Hackultet.

U 2025. godini Nacionalni CERT je provodio aktivnosti i sudjelovao u projektima: e-Sveučilišta, BraAIn i CroQCI.

Organizirana je druga ConCERT konferencija koja je okupila stručnjake iz područja kibernetičke sigurnosti kako bi razmijenili znanje o trenutnoj situaciji upodručju kibernetičke sigurnosti u Hrvatskoj i svijetu te stekli znanja o korisnim alatima koji se mogu koristiti u praksi.

Povodom Dana sigurnijeg interneta, s Centrom za sigurniji internet, HAKOM-om i Udrugom Suradnici u učenju održana je tematska konferencija "Potraga za boljim internetom". Cilj konferencije bio je uputiti snažnu poruku o važnosti prevencije elektroničkog nasilja, zaštite osobnih podataka djece, stvaranja sigurnog virtualnog okružja te dostupnosti kvalitetnih internetskih sadržaja za djecu i mlade.

Bilježimo porast posjeta portalu Nacionalnog CERT-a (http://www.cert.hr) sa 192 502 na 323 417, na kojem je objavljeno 95 novosti iz područja kibernetičke sigurnosti. Povećan je broj posjetitelja i pratitelja na društvenoj mreži Facebook @CERT.hr – 2423 pratitelja.

U porastu je interes medija za djelovanje Nacionalnog CERT-a koji je sudjelovao u brojnim gostovanjima, intervjuima i izjavama za časopise te tiskane i digitalne medije. Uz medijsku pojavnost djelatnici Nacionalnog CERT-a održali su brojne webinare, gostovanja na konferencijama i predavanja s ciljem podizanja svijesti građana o kibernetičkoj sigurnosti.

Nacionalni CERT je u 2025. godini ostvario značajne pomake na području nacionalne i međunarodne suradnje, medijske prisutnosti, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

Miro Đuzel
Pomoćnik ravnatelja za Sektor – Nacionalni CERT

1. Mjere Nacionalnog CERT-a

Usluge Nacionalnog CERT-a besplatne su i dostupne široj javnosti, a djelovanje se financira iz sredstava koja osigurava Ministarstvo znanosti, obrazovanja i mladih, a dijelom Europska unija kroz razne EU projekte.

Tijekom 2025. godine Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave kibernetičkih incidenata i smanjenja šteta pri njihovom nastanku.

1.1. Proaktivne mjere

Proaktivnim mjerama Nacionalni CERT djeluje prije incidenata i drugih događaja koji mogu ugroziti sigurnost informacijskih sustava, a u cilju sprečavanja ili ublažavanja mogućih šteta.

- **diseminacija informacija iz područja kibernetičke sigurnosti** - izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- **praćenje tehnologija iz područja kibernetičke sigurnosti** - izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima;
- **praćenje i objavljivanje novosti u vezi kibernetičke sigurnosti**;
- **provjera ranjivosti za ustanove članice CARNET mreže**;
- **izdavanje elektroničkih certifikata za ustanove članice CARNET-a** (poslužiteljskih i klijentskih);
- sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacija koje pristupaju sustavu eMatica;
- **unapređenje svijesti o značaju kibernetičke sigurnosti** - organiziranje i provedba aktivnosti podizanja svijesti o kibernetičkoj sigurnosti;
- **edukacija i obuka o kibernetičkoj sigurnosti**;
- **održavanje predavanja i webinara o sigurnosti na internetu**;
- sudjelovanje u televizijskim i radijskim emisijama;
- sudjelovanje na predavanjima u sklopu konferencija i radionica.

1.2. Reaktivne mjere

Reaktivnim mjerama odgovara se na incidente u Republici Hrvatskoj te na druge događaje koji mogu ugroziti kibernetičku sigurnost javnih informacijskih sustava u Republici Hrvatskoj.

- **postupanje s kibernetičkim incidentima** - obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);
- **koordinacija rješavanja značajnijih incidenata** - obrada incidenata sukladno Zakonu o kibernetičkoj sigurnosti;
- **sigurnosna upozorenja**;
- prikupljanje podataka o kompromitiranim računalima i njihovim aktivnostima s izvora na internetu te njihova analiza;
- prikupljanje i analiza podataka o napadima dobivenih iz sustava ili senzora;
- Abuse služba CARNET mreže.

2. Stanje kibernetičkih incidenata i statistike

2.1. Statistika o obrađenim incidentima

U 2025. godini zabilježeno je **1513 kibernetičkih incidenata**, što je značajni porast u odnosu na godinu prije. Vodeći tipovi incidenata su: phishing napad, neželjene poruke i ostale vrste financijski motiviranih prijevara.

2025. godine ažurirana je Nacionalna taksonomija kibernetičkih incidenata te je došlo do značajnih promjena u kategorizaciji incidenata. Primjerice incidenti tipa scam i spam su postali jedna kategorija „Neželjene poruke“ te su incidenti tipa Phishing, Malver, Spam URL i C&C sada postali spojeni u jednu kategoriju „Napadačka infrastruktura“. Razlog promjene su pojednostavljenje taksonomije i dodavanje novih vrsta incidenata radi bolje klasifikacije. Taksonomija je „živi“ dokument i ona će se mijenjati ovisno o promjenama metoda napadača.

U odnosu na prošlu godinu zabilježeno je povećanje broja prijava računalno kibernetičkih incidenata za 35,94 %. Pretpostavka je da je do povećanja došlo uslijed rezultata kampanji, edukacija i ostalih aktivnosti podizanja svijesti građana, veće medijske i javne zauzetosti za teme iz područja kibernetičke sigurnosti i posebno sigurnosti i zaštite krajnjih korisnika. Također, stalni trend porasta broja prijava i obrađenih incidenata rezultat je veće javne vidljivosti Nacionalnog CERT-a, ali i neprestanog usavršavanja niza alata za detekciju kompromitacija i dodavanje novih izvora informacija o prijetnjama i incidentima. Zbog velike ovisnosti o tehnologijama i sve sofisticiranijih metoda napadača, u narednim godinama potencijalno se može očekivati trend laganog povećanja ukupnog broja obrađenih incidenata.

Phishing napadi ostaju kao vodeći tip incidenata, u skladu s trendom prethodnih godina. Najveću promjenu vidimo u „Ostalim vrstama financijski motiviranih prijevara“, gdje bilježimo porast broja incidenata sa 12 na 277. Riječ je o incidentima kao što su sextortion prijevare, lažne internetske trgovine, „work from home” i investicijske prijevare. Navedena statistika nam ukazuje na činjenicu da se napadači sve više okreću oblicima prijevare koje će im donijeti financijsku dobit.

U kategoriji neželjene poruke također vidimo velik porast sa 150 na 283 što je porast za 88,67 %. Razlog tome je povećan broj prijava takvih vrsta incidenata od strane građana što pripisujemo većoj javnoj vidljivosti Nacionalnog CERT-a kroz održane prezentacije te objavama na mrežnim i društvenim stranicama.

Prikaz incidenata po tipu u 2025. godini

Phishing napad	478	▲
Neželjene poruke	283	▲
Ostale vrste financijski motiviranih prijevara	277	▲
Napadačka infrastruktura	187	▼
Pogađanje pristupnih podataka	84	▼
Neovlaštena izmjena sadržaja	66	▲
Poslovne prijevare	38	▲
Krađa pristupnih podataka	23	▼
Ispad usluge	20	▲
Kompromitiran uređaj	16	▼
Uskraćivanje usluge	9	▼
Ostalo	8	▲
Ucjenjivački napadi	7	▲
Pokušaj iskorištavanja ranjivosti	6	-
Kompromitiran informacijski sustav	5	▲
Krađa podataka	3	▲
Prikupljanje informacija	3	▼
UKUPNO	**1513**	▲

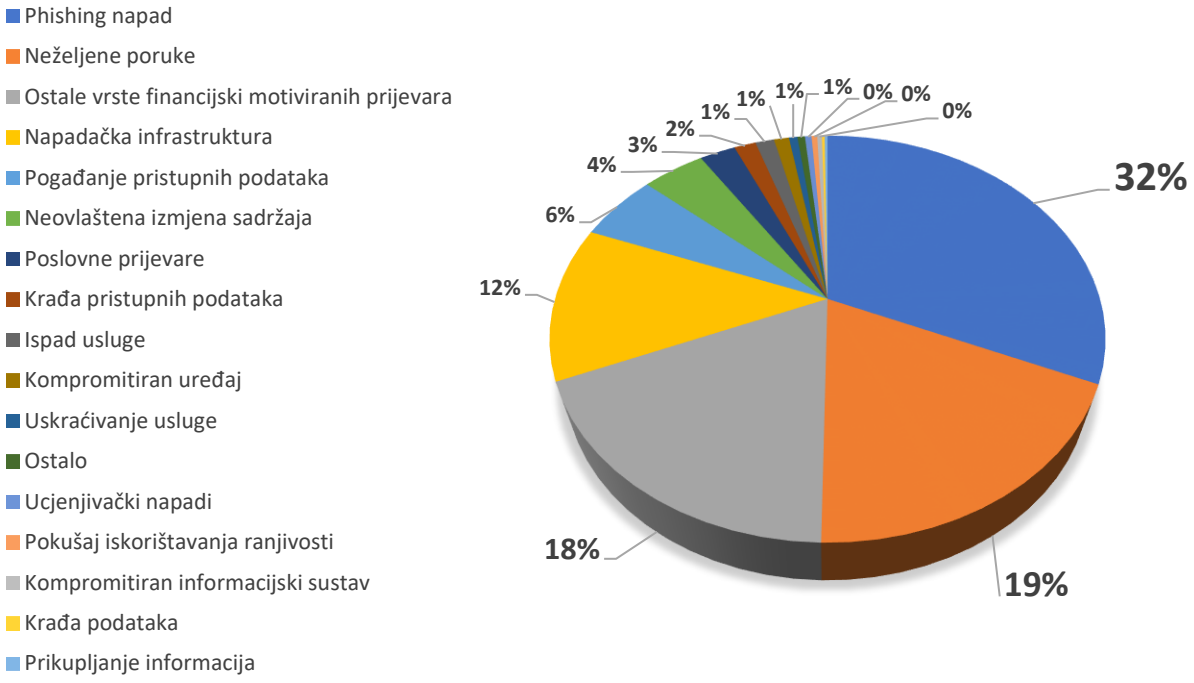
Prema trendu kretanja tipova incidenata vidljivo je da je veći dio kategorija u rastu, kao i sveukupni broj incidenata.

Bez obzira na ukupan broj incidenata u pojedinoj godini, potrebno je uzeti u obzir vektore napada, tematike kojima se napadači bave, ciljane skupine korisnika i pratiti trendove u drugim zemljama. Svake godine bilježi se sve više novih taktika napadača stoga je važno neprestano biti na oprezu i korisnike educirati o opasnostima koje dolaze s interneta.

2.2. Raspodjela incidenata po tipu

Sljedeći grafikon prikazuje udjele incidenata po tipu u 2025. godini, koji su zabilježeni u sustavu za obradu incidenata.

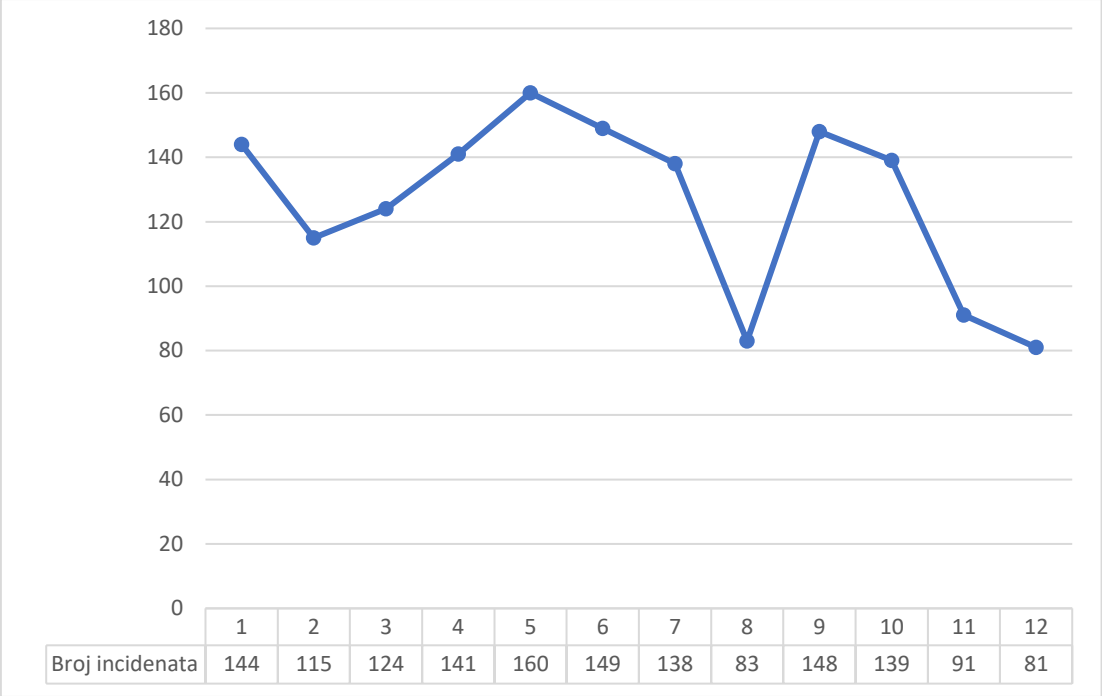
Raspodjela incidenata po tipu u 2025. godini



Prijave incidenata zaprimljene su putem adrese elektroničke pošte za prijavu incidenata, korištenjem OSINT metoda i od vanjskih izvora kroz automatizirane softvere za obradu incidenata.

2.3. Trendovi pojave incidenata u 2025. godini

Sljedeći grafikon prikazuje broj incidenata obrađenih u Nacionalnom CERT-u na mjesečnoj osnovi, koji su zabilježeni u sustavu za obradu incidenata.



	1	2	3	4	5	6	7	8	9	10	11	12
Broj incidenata	144	115	124	141	160	149	138	83	148	139	91	81

Mjesečni prikaz broja obrađenih incidenata

Na grafičkom prikazu vidljiva su dva skoka u broju incidenata - u svibnju i rujnu.

Prvi skok u svibnju je zabilježen zbog povećanog broja phishing kampanja, a najčešće su bile prijavljene: phishing kampanje koje imitiraju odvjetnička društva s malicioznim privitkom, phishing kampanje koje imitiraju sustav e-dozvola te smishing kampanje koje preuzimaju kontrolu nad WhatsApp računima korisnika. Za sve navedene kampanje Nacionalni CERT je izdao upozorenja.

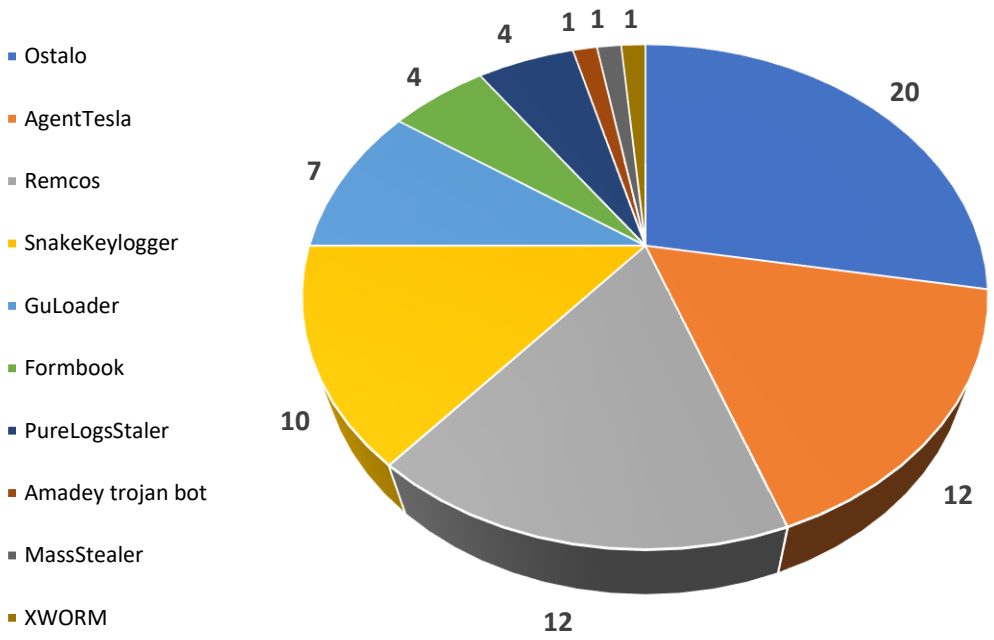
Razlozi povećanog broja incidenata u rujnu su također bile phishing kampanje, a u navedenom mjesecu su najaktualnije bile kampanje koje imitiraju HZZO, Ministarstvo unutarnjih poslova i kampanje koje su uvjeravale građane da su zaradili na trgovanju kriptovalutama imitirajući agente trgovačkih platformi ili financijskih ustanova.

2.4. Vrste malvera

U 2025. godini otkriveno je preko 100 uređaja zaraženih malverom. Zaprimljeno je i analizirano 72 prijave malvera, dok se u ostalim slučajevima radilo o obavijestima o kompromitaciji iz vanjskog izvora koje su proslijeđene vlasnicima zaraženih sustava, incidentima kod kojih je žrtva sama obavila analizu malvera i javila rezultat analize te kompromitiranim web sjedištima. Broj zaraženih uređaja po tipu malvera vidljiv je u tabličnom prikazu ispod. Većina malvera bila je distribuirana putem elektroničke pošte ili preuzimanjem sumnjivih i neprovjerenih softvera.

Tablični prikaz malvera

Obitelj malvera	Broj zaraženih uređaja
Ostalo	20
AgentTesla	12
Remcos	12
SnakeKeylogger	10
GuLoader	7
Formbook	4
PureLogsStaler	4
Amadey trojan bot	1
MassStealer	1
XWORM	1



Prikaz malvera po tipu

Nacionalni CERT analizirao je 72 malvera, najčešće distribuiranih putem elektroničke pošte. Većina malvera bila je "stealer" pri čemu dominiraju vrste malvera poput AgentTesla, Remcos malvera, SnakeKeylogger-a. U odnosu na prethodnu godinu, zabilježen je mali porast u korištenju .iso i .zip datoteka za distribuciju malvera. Primijećena je i česta upotreba NSIS installera za uspostavu različitih stealera, ne samo u okviru AgentTesle, već i u drugim obiteljima malvera. Napadači su unutar svog modus operandi najčešće imitirali privatne tvrtke i državne institucije što ukazuje na prilagodljivost i raznolikost određenih napadača i njihovih strategija prema trendovima.

S obzirom na to da se većinom šire “stealer” malveri koji kradu korisničke podatke kao one za prijave na web stranice, prijavu u sustav i slično - predlažemo hitno skeniranje računala antivirusnim programom te izmjenu zaporki u slučaju kompromitacije. Navedeni malveri ciljaju zapamćene zaporke u preglednicima o čemu smo objavili dokument.

2.5. Registrirani botovi u Republici Hrvatskoj

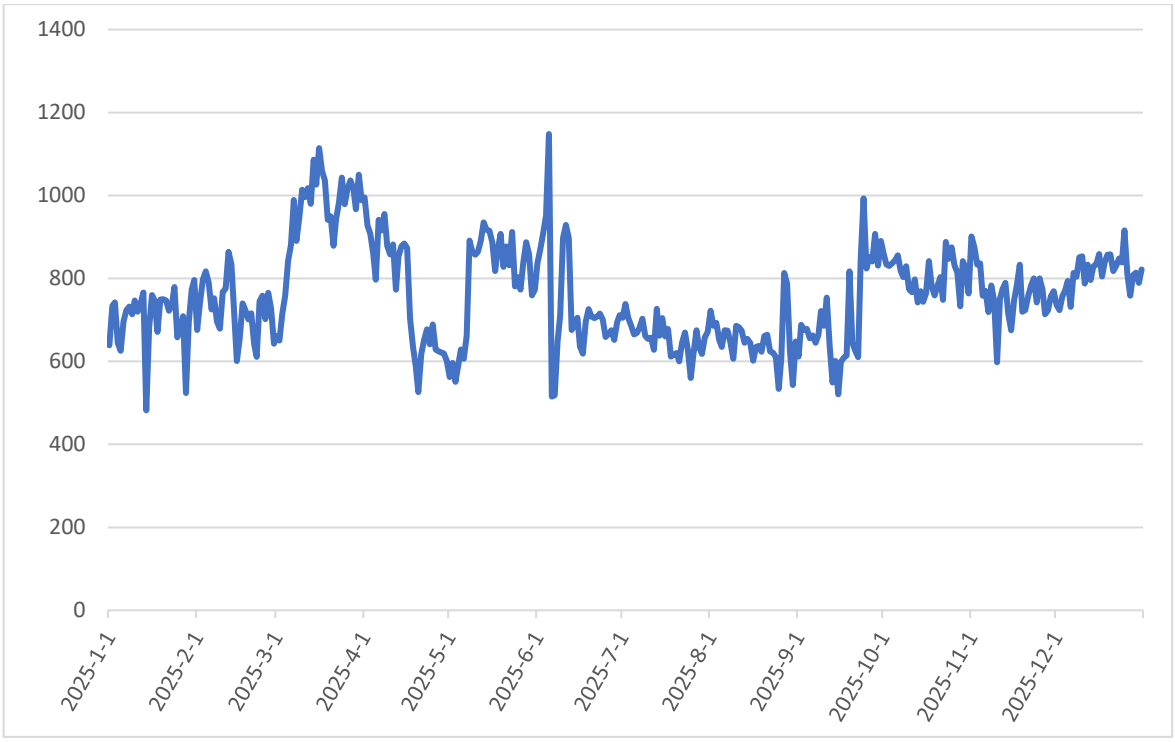
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani nadležnim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). U odnosu na 2024. godinu, u 2025. godini **smanjio se broj registriranih zaraženih računala u Hrvatskoj**. Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2025. godine iznosi **126098**, što je **smanjenje od 33,37 % u odnosu na 2024. godinu**.

Broj otkrivenih *botova* prikazan ovim statističkim podacima temelji se na vanjskim izvorima. Podaci ne odražavaju stvaran broj zaraženih korisničkih računala, no prikazuju trend i daju okvir stvarnog stanja.

U tablici u nastavku prikazano je deset najčešće prijavljivanih *botova* prema tipu (vrsti zlonamjernog sadržaja) u 2025. godini, koji su bili proslijeđeni davateljima internetskih usluga.

Deset najčešće prijavljivanih botova u RH

android.badbox2	29432
android.badbox	20400
android.vo1d2	14905
socks5_systemz	12620
andromeda	12344
pseudo_manuscrypt	4831
android.vo1d	4502
badbox	3816
vipersoftx	3375
adload	2802



Broj zabilježenih botova po danima u 2025. godini

Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću oko **758 *botova* dnevno**, što je manje u odnosu na prošlu godinu. Srednja vrijednost broja *botova* po danu za 2024. godinu iznosila je 1045 što je **smanjenje za više od 27 %**.

2.6. Statistika o obrađenim incidentima CARNET Abuse službe

Služba **CARNET Abuse** bavi se incidentom ako je izvor incidenta korisnik CARNET mreže (ustanova članica ili korisnik AAI@EduHr elektroničkog identiteta). Tijekom 2025. godine, služba CARNET Abuse obradila je ukupno 1350 incidenata. Broj incidenata se povećao za gotovo 44 % u odnosu na prošlogodišnjih 940. I ove godine se većina incidenata (gotovo 58 %) odnosi na **povredu autorskih prava** (distribucija datoteke putem BitTorrent protokola koja je zaštićena autorskim pravom), unatoč povećanju broja takvih incidenata njihov udio se smanjio (u usporedbi sa 72 % u 2024. godini), pretpostavljamo da je uzrok smanjenju temeljita obrada takvih incidenata zbog čega se korisnici suzdržavaju od ponavljanja incidenata. Drugi najčešći incident je **slanje neželjene pošte**. U slučaju slanja neželjene pošte, kao i u većini ostalih slučajeva, korisnike se najčešće savjetuje da skeniraju računalo i očiste ga od zlonamjernog sadržaja. Suradnjom s ostalim pružateljima internetskih usluga (eng. Internet Service Provider – ISP) u Hrvatskoj, dio incidenata obrađuje se kod davatelja usluge koju pojedini korisnik koristi.

3. Značajni događaji po kvartalima

1. kvartal	**Obrađeno je 385 kibernetičkih incidenata**
#385 incidenata **#fakeCaptcha #malver**	U prvom kvartalu 2025. godine bile su aktualne phishing kampanje kojima se distribuirao Lumma stealer malver. Klikom na poveznicu prikazala bi se lažna Captcha i upute za pokretanje malvera. Cilj je bila krađa podataka iz preglednika. Također su bile zaprimljene prijave phishing poruka koje su sadržavale maliciozni privitak (SnakeKeylogger Stealer, GuLoader, PureLogs, Purecrypter, VIPKeylogger).
#digital skimming	Detektirane su kompromitirane online trgovine i web stranice, na .hr domenama, na kojima je bio postavljen digitalni skimmer, odnosno spam sadržaj. Skimmer nije bio ispravno konfiguriran pa nije došlo do krađe bankovnih ili osobnih podataka. Iz vanjskog izvora zaprimljena je prijava o potencijalno kompromitiranom uređaju jednog Hrvatskog ISP-a.
#kompromitacija	Nacionalni CERT je zaprimio prijave ucjenjivačkih kampanja povezanih s jednim kripto novčanikom na kojem je bilo uplata. Nastavljene su scam kampanje koje imitiraju policijske službenike koji traže odgovor na priloženi sudski poziv ili tužbu. Zaprimljene su prijave lažnih online trgovina gdje se isporučuje roba manje vrijednosti ili se uopće ne isporučuje.
#lažne investicije **#phishing**	Iz vanjskog izvora zaprimljene su prijave potencijalno kompromitiranih korisničkih računa djelatnika unutar CARNET mreže. Radi se o računima jedne visokoškolske ustanove, više škola i dviju agencija iz sustava obrazovanja. Zaprimljena je prijava o kompromitaciji korisničkog računa e-pošte visokoškolske ustanove s kojeg se šalju phishing poruke koje sadrže maliciozne poveznice. Maliciozne poveznice preusmjeravaju žrtve na phishing stranicu koja imitira prijavu u AAI@Edu sustav. Phishing stranica ima za cilj krađu pristupnih podataka. Uočeni su postavljeni zavaravajući oglasi na društvenim mrežama u kojima se imitiraju novinarski portali, gdje se poziva na lažne

	investicije. U jednom slučaju radilo se o ulaganju u energetsku tvrtku.
#curenje podataka	Aktualne su phishing kampanje koje ciljaju korisnike online oglasnika i kurirskih službi. Također su aktualne phishing i smishing kampanje u kojima se traži unos podataka o kartici ili korisničkog imena i lozinke te MFA podataka za pristup mobilnom, odnosno digitalnom bankarstvu.
#ranjivosti	Iz vanjskog izvora zaprimljena je prijava o UDP flood DDoS napadu na jednu školu. Anti DDoS zaštita je mitigirala napad. Zabilježeno je nekoliko prijava za lažnu reklamu na društvenoj mreži koja poziva na učenje stranog jezika. Žrtve se preusmjeravaju na maliciozne web stranice u kojima se traži unos kontakt podataka kako bi kasnije mogli biti kontaktirani od strane napadača. Poslana je obavijest korisnicima o potencijalnom curenju podataka tvrtke Oracle, a ista je objavljena i na web stranicama Nacionalnog CERT-a. Detektirane su kritične ranjivosti CVE-2024-55591, CVE-2025-0282 i CVE-2025-0283 na Fortiguard i Ivanti sustavima. Poslane su obavijesti te su izdana upozorenja.

2. kvartal	**Obrađeno je 450 kibernetičkih incidenata.**
#450 incidenata	Zaprimljene su phishing i smishing poruke koje imitiraju tvrtku iz energetskog sektora. Poruke sadrže maliciozne poveznice koje za cilj imaju krađu novca, osobnih podataka kao i podataka bankovnih kartica. Izdano je upozorenje za građane.
#phishing	
#malver	Zaprimljene su prijave phishing poruka koje imitiraju sustav e-Dozvola. Phishing poruke sadrže maliciozni privitak koji za cilj ima krađu lozinki spremljenih u preglednicima. Poslane su prijave prema izvoru incidenta te C2 poslužitelju. Izdano je upozorenje za građane. Zabilježena je kampanja phishing poruka koje imitiraju odvjetnička društva. Navedene poruke sadrže malicioznu poveznicu koja pokreće automatsko preuzimanje malicioznog

	softvera. Maliciozni softver za cilj ima eksfiltraciju podataka. Izdano je upozorenje za građane.
#javno Dostupni servisi	Iz vanjskog izvora zaprimljena je prijava o javno dostupnim VNC instancama za koje je poslana obavijest pružateljima internetskih usluga.
#lažne online trgovine	Zaprimljene su phishing poruke koje sadrže maliciozni privitak (GuLoader, AgentTesla, PureLogs/SNAKE, RemCos). Zaprimljene su prijave lažnih online trgovina. U nekoliko slučaja napadači su reklamirali trgovine na društvenim mrežama, koristeći AI generirane fotografije kako bi djelovali uvjerljivo i navodili rasprodaju zbog zatvaranja trgovine.
#IM phishing	Primijećena je phishing kampanja lažnih poruka, koje su se širile mobilnim aplikacijama za razmjenu poruka u stvarnom vremenu, u kojima se napadač predstavljao kao dijete u nevolji i kroz komunikaciju tražio uplatu novca za što je izdano upozorenje.
#kompromitirane kartice	Detektiran je popis potencijalno kompromitiranih bankovnih kartica građana RH za koji su poslane obavijesti bankama.
#ransomware	Prijavljen je ransomware napad na ustanovu iz obrazovnog sektora. Radilo se o Lockbit3 ransomwareu koji je onemogućio pristup internetu i slanju elektroničke pošte. Pružena je tehnička i savjetodavna pomoć. Sustav je uspješno oporavljen podizanjem nove infrastrukture.
#DDos	Više IP adresa fakulteta i škola sudjelovalo je u DNS DDoS amplifikacijskim napadima uslijed pogrešno konfiguriranih DNS poslužitelja.
#WorkFromHome	Zaprimljeno je više prijava phishing poruka koje se dijele preko aplikacije za instant dopisivanje. Phishing poruka poziva na glasanje na natjecanju, a klik na phishing poveznicu vodi na stranicu dizajniranu s ciljem prikupljanja pristupnog koda pomoću kojeg napadači ukradu sesiju aplikacije. Potom

	napadači kontaktima s aplikacije šalju poruke i traže ih uplatu novca. Izdano je upozorenje za građane. Iz vanjskog izvora zaprimljena je prijava o DDoS napadima na dvije škole. CARNET je detektirao napade te ih uspješno mitigirao. Zabilježene su prijave Work from Home financijske prijevare u kojoj se oglasi za posao distribuiraju društvenim mrežama koristeći imena legitimnih brendova, nakon čega se šalju radni zadaci, uplaćuje se novac putem lažne platforme, dok su za nastavak rada potrebne veće uplate od strane radnika. Zaprimljene su prijave phishing poruka s phishing URL-om koje imitiraju domaćeg pružatelja usluga udomljavanja s tematikom isteka domene. Zaprimljena je prijava Booking prijevare gdje se stranica predstavlja kao platforma za rezervaciju smještaja s ciljem prijevare i krađe novčanih sredstava i podataka korisnika.
3. kvartal **#369 incidenta** **#phishing** **#investicijska ulaganja** **#CVE** **#smishing**	**Obrađeno je 369 kibernetičkih incidenata.** Zaprimljene su prijave prijevare rada od kuće gdje se žrtve navodi na obavljanje zadataka putem interneta na lažnim platformama za zapošljavanje kojima je cilj krađa novčanih sredstava. Povećan je broj prijava na temu iznajmljivanja smještaja. Napadači putem lažne platforme daju u najam postojeće apartmane i žrtve su prevarene na način da misle da su uspješno rezervirali i platili smještaj, dok vlasnik tvrdi da ne izdaje putem lažne platforme. Zaprimljene su prijave građana koji su primili pozive od nepoznatih osoba koje se predstavljaju kao agenti trgovačkih platformi ili financijskih institucija. Prevaranti tvrde da su građani ostvarili zaradu trgovanjem kriptovalutama — iako ti građani nikada nisu ulagali u njih. Objavljeno je upozorenje.

#Suradnja	Detektirana je kritična ranjivost na Microsoft SharePoint poslužitelju (CVE-2025-53770) u više ustanova pod nadležnosti Nacionalnog CERT-a. Iskorištavanje ove ranjivosti ("ToolShell") potencijalno omogućuje neautentificiranom napadaču udaljeno izvršavanje proizvoljnog programskog koda i potpuni pristup sadržaju SharePointa. Zaprimljene su prijave postavljenih malicioznih skripti za prikupljanje podataka o bankovnim karticama (digital skimming) na digitalnim trgovinama na .hr domeni. U suradnji s ostalim tijelima RH, prijavljene su phishing kampanje s phishing URL-ovima kompromitiranih korisničkih računa tijela državne uprave. Nacionalni CERT je poslao prijave za gašenje phishing poveznica, dok su informacije o kompromitaciji korisničkih računa proslijeđene CSIRT tijelu pri Nacionalnom centru za kibernetičku sigurnost. U suradnji s MUP-om prijavljena je web stranica koja imitira stranicu kampanje za podizanje svijesti o kibernetičkom kriminalu, kojoj je cilj prikupljanje telefonskih brojeva u svrhu daljnje prijevare.
#ransomware	Iz vanjskog izvora zaprimljena je prijava ransomware napada na jedno hrvatsko visoko učilište. Napadač navodi da je uspješno ostvario pristup te da će eksfiltrirati 70 Gb podataka. Vektor napada je kompromitacija računa djelatnice i poslužitelja na kojem se nalaze administrativne aplikacije i podaci putem otvorenog RDP protokola. Nakon analize zaključeno je kako je samo dio datoteka zaključan te da podaci nisu eksfiltrirani u tom obujmu. Sistem administratoru ustanove su dane savjetodavne i mitigacijske upute kako se napad ne bi ponovio. Zaprimljena je prijava ransomware napada na jedan hrvatski znanstveni institut. Nacionalni CERT u suradnji s NCSC-om i vanjskim izvođačima instituta koordinira rješavanje incidenta. Inicijalna analiza pokazala je da je ransomware zahvatio dio mreže za administrativne poslovne procese uprave. Backup poslužitelj nije bio zahvaćen napadom, no napadač je obrisao

	sigurnosne kopije. Odrađena je izolacija ostatka mreže radi prevencije dodatne štete. Radi se o CRING/GHOST/HsHarada ransomwareu za koji ne postoji dekripcijski ključ. Prikupljeni su dnevnički zapisi radi analize te instalirana sigurnosna rješenja. Prema napravljenoj analizi pretpostavlja se da se radi o zastarjelom Sharepoint poslužitelju kao inicijalnom vektoru napada. Zaprimljena je prijava maliciozne poruke poslane s kompromitiranih računa djelatnice Ministarstva znanosti, obrazovanja i mladih, škole i jednog visokog učilišta. Prijave su proslijeđene nadležnim osobama te su lozinke računa promijenjene. Zaprimljene su prijave lažnih web trgovina na .com, .com.hr ili .hr domenama. Lažne web trgovine oglašavaju se uglavnom putem društvenih mreža te imitiraju poznate modne ili druge brendove. Lažne trgovine nakon narudžbe šalju robu manje vrijednosti, robu koja nije naručena ili reklamirana ili ne pošalju robu uopće. Zaprimljene su prijave smishing poruka koje imitiraju Poreznu upravu te prijavu na NIAS. Napadač od potencijalne žrtve traži unos osobnih podataka i podataka bankovne kartice. Poslane su obavijesti za potencijalno ranjive servise, radi se o SonicWall SSL-VPN ranjivosti. Ranjivost nultog dana omogućuje napadaču pristup sustavu te postavljanje ucjenjivačkog koda. Iz vanjskog izvora zaprimljena je prijava o Citrix ranjivosti (CVE-2025-7775) koja potencijalno napadaču omogućuje izvođenje DOS napada ili izvršavanje proizvoljnog koda (RCE). Aktualna je također smishing kampanja u kojoj se imitira HZZO s ciljem krađe korisničkih podataka i sredstava, za koju je izdano upozorenje. Na komunikacijskom kanalu CSIRT mreže podijeljena je informacija o ranjivosti na Omnissa Workspace ONE UEM | AirWatch MDM (bivši VMWare) on-premise sustavima.

	Navedena ranjivost potencijalnom napadaču omogućuje čitanje povjerljivih podataka bez autentifikacije. Poslane su obavijesti vlasnicima sustava u nadležnosti Nacionalnog CERT-a te je obaviješten CSIRT NCSC-a. Poslana je obavijest za potencijalnu ranjivost CVE-2025-10035 na jednom hrvatskom sustavu. Radi se o ranjivosti deserializacije u License Servlet GoAnywhere MFT-a. Poslane su obavijesti i savjeti za mitigaciju za kritičnu Cisco Secure Firewall VPN te Adaptive security appliance ranjivost (CVE-2025-20333), izdano je i upozorenje. MUP je prijavio phishing mail s phishing URL-om koji imitira sučelje za prijavu u MUP webmail, pri čemu su poslane prijave izvorima incidenta. Zaprimljena je prijava spearphishinga koji je ciljao zamjenika ravnatelja CARNET-a, a radi se o phishing emailu koji sadrži Word dokument s QR kodom na temu plaća i isplate bonusa.

4. kvartal **#311 incidenata** **#phishing URL** **#malver** **#DDoS napad** **#Kompromitirani korisnički računi**	**Obrađeno je 311 kibernetičkih incidenata.** U cijelom kvartalu bile su aktivne smishing i phishing kampanje koje ciljaju korisnike dostavnih službi, pošte, online oglasnika i aplikacija za dopisivanje. Maliciozne poruke sadrže phishing poveznice koje za cilj imaju krađu osobnih podataka, kao i podataka bankovnih kartica. Osim navedenih, tijekom cijelog perioda redovito su zaprimane prijave za lažna investicijska ulaganja u kriptovalute, Work From Home prijevare i stranice koje nude prijevarne novčane zajmove kojima je cilj ostvarivanje financijske koristi. U navedenom razdoblju zaprimljene su i prijave phishing poruka koje sadrže maliciozne skripte ili privitke vrste AgentTesla, RemCos, SnakeKeylogger. Ustanova visokog obrazovanja prijavila je DDoS napad na web stranicu same ustanove. Analizirani su dnevnički zapisi te su na temelju njih pružene savjetodavne usluge u vidu načina zaštite od budućih napada.

#Lockify ransomware	Iz vanjskog izvora smo zaprimili više prijava o kompromitiranim korisničkim računima fakulteta, te je zaprimljena prijava i o kompromitaciji korisničkog računa jedne škole. Svi kompromitirani računi su se koristili za daljnje napade odnosno slanje malicioznih poruka.
#Cisco ranjivost	Zaprimljena je prijava ransomware napada na objekt koji nudi smještaj, dostavljene su datoteke na analizu. Radilo se o Lockify ransomwareu za koji nije javno objavljen ključ za dekripciju. Pružena je savjetodavna pomoć u obliku mjera mitigacije napada, oporavka i dodatnih mjera zaštite. Poslane su obavijesti za ranjivost Cisco Secure Firewall VPN te Adaptive security appliance, CVE-2025-20333, CVE-2025-20363, CVE-2025-20362. Poslane su obavijesti o potencijalno ranjivim Redis sustavima. Radi se o CVE-2025-49844 kritičnoj ranjivosti. Poslane su obavijesti o ranjivostima i kibernetičkom incidentu tvrtke F5, te su dostavljene mitigacijske mjere. Poslane su obavijesti i o WSUS (Windows Server Update Service) ranjivosti CVE-2025-59287, koja potencijalnom napadaču omogućuje izvršavanje proizvoljnog koda. Zabilježena je prijava ustanove visokog obrazovanja o kompromitaciji poslužitelja uslijed koje je napadač uklonio legitiman sadržaj te na njegovo mjesto postavio maliciozni sadržaj. Nakon što je incident detektiran, poslužitelj je ugašen kako bi se poduzele mjere zaštite. Analizom forenzičkih artefakata otkriveno je kako je napadač najvjerojatnije ostvario pristup preko ranjivog WordPress dodatka te je postavio backdoor.
#React2shell	Zaprimljena je prijava o ransomware napadu na poslužitelja jedne visokoškolske ustanove. Radilo se o poslužitelju koji evidentira ulaz i izlaz iz prostorija. Odmah nakon detekcije napada poslužitelj je uklonjen s mreže te su provedene reinstalacija i vraćanje podataka iz sigurnosne kopije, čime su

	onemogućene detaljne forenzičke radnje. Nakon vraćanja podataka primijenjene su dodatne zaštitne mjere. Poslane su prijave za kritičnu ranjivost React2Shell (CVE-2025-55182) u React Server Components (RCS) Flight protokolu koja omogućuje udaljeno izvršavanje koda bez autentifikacije u React i Next.js aplikacijama. Za navedenu ranjivost izdano je upozorenje. Poslane su prijave za kritičnu ranjivost WatchGuard Firewera (CVE-2025-14733) koja omogućuje udaljenom, neautentificiranom napadaču izvršavanje proizvoljnog koda. Poslane su prijave za kritičnu ranjivost u MongoDB (CVE-2025-14847) koja omogućuje udaljenom napadaču čitanje osjetljivih podataka.

4. Usluge CARNET-ovog Nacionalnog CERT-a

4.1. CERT spamblok

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu Nacionalni CERT nudio je uslugu CERT SPAMBLOK koja predstavlja sustav DNSBL (eng. *Domain Name Server Blacklist*) ili RBL sustav (eng. *Real Time Blacklist*) i bila je dostupna široj javnosti kao dodatak (*plugin)* za poslužitelje e-pošte. Svrha **CERT SPAMBLOK** usluge bila je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvatske i regije (tzv. *spameri*), a koji često nisu obuhvaćeni poznatim globalnim listama. **CERT SPAMBLOK** nije zamjena za poznate liste kao što su *Spamhaus*, *SpamCop*, *Sorbs* i sl.

Praćenjem pokazatelja korištenja usluge vidljivo je da je dodatak bio postavljen na poslužiteljima e-pošte i mjesečno stavljao na crnu listu u prosjeku **73** jedinstvene IP adrese i **8** jedinstvenih domena, a broj korisničkih upita za pristigle poruke elektroničke pošte u mjesečnom prosjeku iznosio je **1 406 714**.

cert spamblok

Napomena: **CERT SPAMBLOK** usluga ugašena je od **1. siječnja 2026.** godine.

4.2. CERT CVE

CERT CVE korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava. Uz to, korisnicima omogućava brže pretraživanje poznatih ranjivosti prema specifičnim kriterijima kao što su proizvođač, CWE (eng. *Common Weakness Enumeration*) oznaka te ID oznaka.

Usluga je namijenjena svim korisnicima, a posebno onima koji rade u području kibernetičke sigurnosti te im je potrebna sažeta informacija o poznatim ranjivostima proizvođača i proizvoda koje su sami odabrali u obliku personalizirane poruke elektroničke pošte.

Informacije o ranjivostima moguće je podijeliti prema CVSS (eng. *Common Vulnerabilities Scoring System*) ocjeni što korisniku dopušta da sadržaj svojeg izvještaja kroji sukladno svojim prioritetima. Izvještaj u obliku poruke elektroničke pošte sadrži popis poznatih ranjivosti te poveznice do detaljnijih informacija o istima, a u slučaju izmjene informacija o pojedinačnoj

ranjivosti u NVD (eng. *National Vulnerability Database*) bazi, korisniku se o njima šalje informacija.

Prema pokazateljima korištenja usluge u 2025. godini ukupan broj korisnika usluge je više od **516**, a ukupan broj posjeta stranici je **41 186**.

4.3. PiXi - Platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima

S ciljem jačanja nacionalne otpornosti na kibernetičke prijetnje i usklađivanja s europskim regulativama, Hrvatska akademska i istraživačka mreža – CARNET 2024. je razvila te u 2025. kontinuirano nadograđuje Platformu PiXi, nacionalnu platformu za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima.

Riječ o platformi koja unaprjeđuje razmjenu podataka o kibernetičkim prijetnjama i incidentima na nacionalnoj razini, s ciljem povećanja razine pripravnosti i učinkovitog odgovora na sve sofisticiranije kibernetičke napade i ugroze.

Platforma je namijenjena obveznicima Zakona o kibernetičkoj sigurnosti, Uredbe o digitalnoj operativnoj otpornosti za financijski sektor (DORA Uredba), nadležnim tijelima za provedbu zahtjeva kibernetičke sigurnosti, nadležnim tijelima za provedbu posebnih zakona, nadležnim CSIRT tijelima i jedinstvenoj kontaktnoj točki te im omogućava ispunjavanje zakonskih obaveza izvještavanja o kibernetičkim incidentima i prijetnjama. **Pristup Platformi PiXi imaju isključivo ovlaštene osobe** koje se prijavljuju putem Nacionalnog identifikacijskog i autentifikacijskog sustava (NIAS), koristeći vjerodajnice visoke ili značajne razine sigurnosti.

Korištenjem PiXi platforme ubrzan je i pojednostavljen postupak prijave incidenata za sve obveznike regulative koja uređuje područje kibernetičke sigurnosti te su postavljeni temelji učinkovite i koordinirane zaštite nacionalnog kibernetičkog prostora. Platforma predstavlja nacionalnu točku razmjene informacija i izvještavanja o kibernetičkim prijetnjama, a njezino uvođenje omogućava svim obveznicima propisa koji uređuju kibernetičku sigurnost u Hrvatskoj da pokrenu pravovremeni i učinkoviti odgovor na kibernetičke prijetnje koje mogu ugroziti poslovanje te društvenu i ekonomsku stabilnost.

4.4. CERT iffy

CERT iffy je alat s pomoću kojega građani mogu sami provjeriti internetsku trgovinu odnosno sadrži li obilježja lažnog weba. Sve što korisnici trebaju napraviti je upisati ili kopirati URL sumnjive internetske trgovine i pritisnuti gumb za provjeru. Važno je napomenuti kako su rezultati analize informativnog karaktera te se korisnicima savjetuje da dodatno samostalno provjere internet trgovine s pomoću indikatora koje će pronaći na stranicama servisa, a odluku o kupovini donose samostalno. U 2025. godini servis je koristilo više od **22 000** korisnika što je **povećanje za otprilike 10 %** u odnosu na 2024. godinu, a provjeren je **37 191** URL što predstavlja **povećanje od čak 89 %.** Na popisu trgovina s obilježjima lažnih internetskih trgovina nalazi se više od **44 000** URL-ova, od kojih otprilike 2050 cilja građane Republike Hrvatske. Broj aktivnih lažnih internetskih trgovina se konstantno mijenja što otežava utvrđivanje njihovog točnog broja.

4.5. Sigurnost CARNET usluga

Tijekom 2025. godine Služba za sigurnost usluga i infrastrukture CARNET-ovog Nacionalnog CERT-a provodila je sljedeće aktivnosti s ciljem povećanja razine sigurnosti CARNET-ovih usluga i infrastrukture.

- prikupljanje i analiza sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija i usluga CARNET-a;
- usluga izdavanja elektroničkih certifikata (TCS);
- provođenje odredaba Programa sigurnosti;
- uvođenje novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNET-a;

- redovita provjera ranjivosti (eng. *Vulnerability Scanning*) ustanova članica CARNET mreže;
- analiza stanja sigurnosti CARNET-ovog IP adresnog prostora ovisno o ugrozama;
- analiza stanja sigurnosti CARNET ustanove radi unaprjeđenja sigurnosti.

U sklopu tih aktivnosti Nacionalni CERT je:

- provodio penetracijska testiranja (19) važnih CARNET-ovih usluga u sklopu implementacije Programa sigurnosti u CARNET-ove poslovne procese;
- provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET.

4.5.1. Provjera ranjivosti

Nacionalni CERT nudi uslugu redovite provjere ranjivosti (eng. *Vulnerability Scanning*) ustanova članica **CARNET** mreže. Redovita provjera ranjivosti obavlja se periodički svaka tri mjeseca, a koristi je 48 ustanova iz sustava obrazovanja, visokog obrazovanja, kulture te neka državna tijela unutar **CARNET** mreže. U 2025. godini provedene su ukupno 144 provjere ranjivosti.

Stručnjaci **Nacionalnog CERT-a** redovne provjere ranjivosti provode korištenjem specijaliziranih alata i samo s određenih računala s istim IP adresama. Rezultati te provjere šalju se odgovornim osobama ustanova u obliku izvještaja koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje koje korisnicima mogu pomoći pri uspješnijem održavanju njihovih mreža.

4.5.2. Trusted Certificate Service – TCS

Od travnja 2020. godine u suradnji s organizacijom **GÉANT** (prije DANTE i TERENA), CARNET nudi uslugu izdavanja elektroničkih certifikata. Izdavatelj certifikata je neprofitna javna tvrtka **HARICA** s kojom je GÉANT zajednica sklopila ugovor. Akademskoj i obrazovnoj zajednici je dana mogućnost besplatnog izdavanja digitalnih certifikata izdanog od validnog CA (*Certificate Authority*).

Vrste certifikata koji se mogu dobiti ovom uslugom su poslužiteljski certifikati, klijentski S/MIME certifikati, *Code Signing* certifikati, *Document Signing* certifikati te *Grid* certifikati za *eScience* projekte. U 2025. godini se 213 ustanova služilo ovom uslugom.

5. Suradnja i djelovanje Nacionalnog CERT-a na međunarodnoj razini

Pored **EU-a** i **NATO-a**, Nacionalni CERT aktivno surađuje te je član sljedećih organizacija:

- **CSIRT mreža** - uspostavljena NIS Direktivom, a čine ju CSIRT-ovi država članica EU, CERT-EU i ENISA te djeluje s ciljem doprinosa razvoju povjerenja između država članica i promicanju brze i učinkovite operativne suradnje.
- **FIRST** - (*Forum of Incident Response and Security Teams*) međunarodna konfederacija CSIRT-ova koji surađuju i zajedno rješavaju kibernetičke incidente te promoviraju programe prevencije.
- **TF-CSIRT** - (*Task Force CSIRT*) radna skupina koja promiče suradnju i koordinaciju između CSIRT-a u Europi i susjednim regijama, istovremeno uspostavljajući veze s relevantnim organizacijama na globalnoj razini i u drugim regijama.
- **TI** - (*Trusted Introducer)* program koji predstavlja pouzdanu okosnicu infrastrukturnih usluga timova i održava listu poznatih, akreditiranih i certificiranih timova prema njihovoj pokazanoj i provjerenoj razini zrelosti. Jedan je od tri elementa koji čine jezgru TF-CSIRT portfelja uz Sastanke radne skupine i TRANSITS. CERT.hr je akreditirani član od 2010. godine.

5.1. Vježba Cyber Coalition 2025

Hrvatska akademska i istraživačka mreža - **CARNET** i **Nacionalni CERT** aktivno su sudjelovali u **NATO** vježbi zaštite NATO-a i nacionalnih računalnih sustava pod nazivom **"Cyber Coalition 25"**. Cilj vježbe je osnažiti koordinaciju i suradnju između članica **NATO** saveza, te poboljšati mogućnosti odvraćanja, obrane i suzbijanja prijetnji u i kroz kibernetički prostor. Nacionalni ciljevi vježbe uključuju uvježbavanje i potvrđivanje postojećih procedura u otkrivanju i postupanju u slučajevima kibernetičkih incidenata.

Cyber Coalition najveća je **NATO** vježba u području kibernetičke obrane. Organiziralo ju je Savezničko zapovjedništvo za transformacije (ACT), a održala se **od 28. studenoga do 5. prosinca 2025.**

Scenariji na vježbi simulirali su ugroze iz stvarnog života kao što su napadi na energetsku infrastrukturu, promet i vojne ciljeve.

CARNET i **Nacionalni CERT** su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u operativnom dijelu, tehničkom dijelu, pravnom scenariju i kriznom komuniciranju. Osim otkrivanja incidenata, provedbe obrambene kibernetičke operacije i oporavka sustava, čime se bavila tehnička obučna skupina, hrvatska provedba uključivala je također operativnu i pravnu

obučnu skupinu. Operativna skupina imala je zadaću koordinacije i osiguranja provedbe vojne operacije u uvjetima degradirane slobode djelovanja u kibernetičkom prostoru, dok je pravna skupina osiguravala donošenje odluka u skladu s međunarodnim pravom i praksom te poduzimanje pravnih mjera protiv počinitelja. Skupina za krizno komuniciranje koordinirala je protok informacija, upravljala medijskom strategijom i osiguravala pravovremeno i točno informiranje javnosti i sudionika.

Republika Hrvatska u vježbi sudjeluje od 2009. godine kao promatrač, a od 2013. kao aktivni sudionik vježbe. Od 2015. godine vježbi su se pridružili i predstavnici iz privatnog sektora i akademske zajednice.

CYBER COALITION 2025

5.2. CSIRT mreža

Mreža **CSIRT-ova** (eng. *CSIRTs Network*) nastala je na temelju Direktive o mrežnoj i informacijskoj sigurnosti (NIS direktiva) iz 2016. godine koju je donijela Europska unija. **NIS** direktiva donesena je s ciljem postizanja visoke razine sigurnosti mreže i informacijskih sustava unutar EU, doprinosa razvoju povjerenja među državama članicama te promicanja brze i učinkovite operativne suradnje. Godišnje se održe tri sastanka Mreže na kojima sudjeluju predstavnici **CERT-ova zemalja članica, ENISA-e, CERT-EU te Europske Komisije**. Na sastancima se predstavljaju rezultati radnih grupa koje su oformljene unutar CSIRT mreže s ciljem unaprjeđenja suradnje, komunikacije i razmjene informacija među CSIRT-ovima Europske unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a te razmjenu znanja i razvoj alata koji se koriste u CSIRT zajednici. Osim ranije spomenutog, na sastancima se redovito izvještava o aktivnostima ENISA-e.


CSIRTs
NETWORK

6. Suradnja i djelovanje Nacionalnog CERT-a na nacionalnoj razini

6.1. Sporazum o poslovnoj suradnji s MUP-om

U 2025. godini nastavlja se suradnja na prevenciji i rješavanju kibernetičkih incidenata i drugih oblika kibernetičkog kriminaliteta između MUP-a i CARNET-a (Nacionalnog CERT-a). Sporazumom koji je obnovljen još krajem 2017. godine nastavlja se suradnja s ciljem očuvanja sigurnosti kibernetičkog prostora Republike Hrvatske. S obzirom na činjenicu da suvremeni način borbe protiv kibernetičkog kriminaliteta, kao osnovni preduvjet uspješnosti, podrazumijeva dijeljenje informacija između relevantnih institucija i visoku razinu tehničkih predznanja, MUP i CARNET suglasno su osigurali suradnju kako bi uvijek bili spremni na kibernetičke izazove kojih je svakim danom sve više.

6.2. Suradnja s FER-om

CARNET-ov Nacionalni CERT nastavlja suradnju s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu, Laboratorijem za sustave i signale (LSS) Zavoda za elektroničke sustave i obradu informacija FER-a. Tijekom 2025. godine provedena su CTF natjecanje iz područja kibernetičke sigurnosti za srednje škole – Hacknite i natjecanje za studente - Hackultet. Za potrebe natjecanja razvijeni su zanimljivi i izazovni sadržaji te platforme za njihovu provedbu. Više o natjecanjima i platformama pročitajte u poglavlju 7.

6.3. Suradnja s Hrvatskom udrugom banaka

Nacionalni CERT je sudjelovao na mjesečnim sastancima Odbora za sigurnost Hrvatske udruge banaka. Djelokrug rada Odbora je organiziranje zajedničkih aktivnosti radi unapređenja informacijske sigurnosti, razvoja sustava upravljanja rizicima nastalih zloupotrebom

informacija i informacijskih kanala te pripremanje i davanje inicijative za formiranje pravne i zakonske regulative informacijske sigurnosti u Hrvatskoj. Međusektorska suradnja vrlo je važna u borbi protiv kibernetičkih incidenata. Sektor bankarstva jedan je od pet sektora za koje je Nacionalni CERT nadležni CSIRT sukladno zakonu. Na sastancima se izvještava o trendovima i eventualnim aktualnim ugrozama u području kibernetičke sigurnosti, a zainteresirane banke mogu se obratiti **Nacionalnom CERT-u** kako bi zaprimale tjedne izvještaje o ranjivim servisima.

U studenom 2025. godine **Nacionalni CERT** sudjelovao je kao partner u nacionalnoj kampanji **„Budimo realni“**, koju je pokrenula Hrvatska udruga banaka (HUB) u suradnji s Ministarstvom unutarnjih poslova (MUP). Kampanja je provedena uoči „Crnog petka“, razdoblja povećanog broja internetskih kupovina te je bila usmjerena na sprječavanje internetskih prijevara i podizanje razine kibernetičke svjesnosti građana o sigurnom korištenju digitalnih usluga. Kroz televizijske spotove i **edukativnu internetsku stranicu**, kampanja je pružila konkretne savjete, primjere iz stvarnog života i edukativne video materijale s ciljem jačanja sigurnosti građana u digitalnom okruženju.

Kampanja „Budimo realni“

6.4. Obilježavanje Europskog mjeseca kibernetičke sigurnosti (ECSM)

CARNET-ov Nacionalni CERT, kao nacionalni koordinator provedbe Europske kampanje **“European Cyber Security Month”** (ECSM), i u 2025. godini aktivno je sudjelovao u obilježavanju Europskog mjeseca kibernetičke sigurnosti s ciljem podizanja svijesti hrvatskih građana o kibernetičkim prijetnjama i sigurnom ponašanju u digitalnom okruženju.

Cilj kampanje bio je podizanje kibernetičke svjesnosti kao alata za obranu od prijetnji potaknutih primjenom umjetne inteligencije. Aktualna istraživanja i statistički podaci ukazuju na to da suvremene kibernetičke prijetnje sve češće ciljaju ljudske emocije, poput ljubavi,

straha ili srama, odnosno potiču hitne reakcije kako bi se umanjila mogućnost racionalnog donošenja odluka. U digitalnom okruženju u kojem brzina često ide u korist napadača, kampanja je promovirala suprotan pristup, naglašavajući važnost usporavanja, povećane svjesnosti i promišljenog odlučivanja.

Potraga za boljim internetom – okrugli stol s učenicima i učenicama

6.5. Dan sigurnijeg interneta 2025.

Povodom Dana sigurnijeg interneta, s HAKOM-om, Centrom za sigurniji internet i Udrugom Suradnici u učenju održana je tematska konferencija "Potraga za boljim internetom". Poseban naglasak je stavljen na okrugli stol s učenicima i učenicama osnovnih i srednjih škola na kojem se raspravljalo o prednostima i opasnostima interneta. Učenici su se složili u jednom – iako internet nudi brojne mogućnosti za učenje i zabavu, važno je da ga znamo koristiti na siguran način. Stručnjaci i djeca razgovarali su o mogućnostima stvaranja sigurnijeg i inkluzivnijeg digitalnog okruženja te prilagodbi društva brzim tehnološkim promjenama kako bi internet postao siguran prostor za komunikaciju i edukaciju. Predstavljen je pregled glavnih aktivnosti i inicijativa usmjerenih na zaštitu djece od digitalnih prijetnji te načini prepoznavanja i rješavanja rizičnih situacija na internetu, a naglašeno je i kako učitelji i nastavnici trebaju biti ukorak s razvojem novih tehnologija kako bi djeci mogli prenijeti znanja potrebna za snalaženje i sigurnije korištenje interneta.

Potraga za boljim internetom – okrugli stol s učenicima i učenicama

6.6. ConCERT

U veljači je održana druga ConCERT konferencija na temu kibernetičke sigurnosti u organizaciji CARNET-ovog Nacionalnog CERT-a na kojoj se okupilo dvjestotinjak stručnjaka iz Hrvatske i Slovenije, koji su razmijenili iskustva i znanja u borbi s kibernetičkim prijetnjama i najboljih odgovora i postupanja uslijed pojave kibernetičkih incidenata. Odaziv na drugu ConCERT konferenciju pokazatelj je povećane svijesti o važnosti zaštite kibernetičkog prostora, otpornosti poslovanja na prijetnje i bržeg odgovora na kibernetičke incidente.

ConCERT konferencija

6.7. Djelovanje putem javnih medija i obraćanja javnosti

Djelovanje putem javnih medija

Nacionalni CERT je tijekom 2025. godine zaprimio brojne medijske upite za koje su pripremljeni informativni članci o temama poput lažnih web trgovina, internetskih prijevara, investicijskih prijevara, zlonamjernih softvera, Europskog mjeseca kibernetičke sigurnosti, projekata i djelovanja Nacionalnog CERT-a. Uz tiskane medije, zabilježena su brojna gostovanja u televizijskim i radio emisijama posvećena temama iz kibernetičke sigurnosti.

Teme kibernetičke sigurnosti i aktivnosti Nacionalnog CERT-a privlače sve veću pozornost medija, pa su tako naši stručnjaci sudjelovali u brojnim medijskim nastupima, a pojam „Nacionalni CERT“ spominje se u čak 376 medijskih objava.

Portal Nacionalnog CERT-a tijekom 2025. godine posjetilo je 200 633 korisnika s ukupno 313 417 posjeta stranice, a objavljeno je 95 novosti iz područja kibernetičke sigurnosti.

Nacionalni CERT u 2025. godini bilježi daljnji porast pratitelja na društvenoj mreži Facebook @CERT.hr – 2423 pratitelja.

6.8 Konferencije, edukacije i mrežni seminari

Predstavnici Nacionalnog CERT-a sudjelovali su na brojnim događanjima na kojima su predstavljene razne teme iz područja kibernetičke sigurnosti od kojih izdvajamo konferencije povodom Dana sigurnijeg interneta, 2nd Cybersecurity Awareness Raising konferenciju u organizaciji ENISA-e u Zagrebu, ConCERT konferenciju te CARNET-ove konferencije za korisnike. Također, izdvojili bismo i edukacije koje su održane na poziv ustanova, te trenažni kamp i selekciju natjecatelja za nacionalni tim koji je predstavljao Hrvatsku na europskom natjecanju iz kibernetičke sigurnosti.

7. CTF natjecanja

7.1. Hacknite

Šesto izdanje hrvatskog CTF natjecanja za srednjoškolce HACKNITE provedeno je od 17. do 19. listopada 2025. godine. Natjecanju su mogli pristupiti samo prijavljeni timovi (ukupno šest osoba – prijavitelj i pet članova tima) s dobivenim korisničkim podacima za pristup natjecanju. Pravo sudjelovanja imali su svi učenici srednjih škola u Republici Hrvatskoj uz mentorstvo svojih profesora kao prijavitelja tima.

Natjecanje je bilo organizirano u obliku CTF-a (Capture the Flag), a cilj mu je proširiti svijest o važnosti primjene sigurnosnih mjera te izbjegavanju i ispravljanju mogućih sigurnosnih propusta u programskom kôdu, postavkama ili nekoj drugoj komponenti računalnog sustava.

Na natjecanje se prijavilo 240 učenika u 48 srednjoškolskih timova iz 26 srednjih škola. Pobjednički tim bio je tim **GO4T** sastavljen od učenika iz Gimnazije i strukovne škole Jurja Dobrile Pazin.

Za sve postojeće i buduće natjecatelje dostupna je Hacknite CTF platforma na kojoj se učenici, nakon registracije svojim @skole.hr računom, mogu pripremati za buduća natjecanja, rješavati zadatke i učiti o kibernetičkoj sigurnosti. Platforma sadrži zadatke sa svih dosadašnjih natjecanja, a učenici mogu pratiti i svoj poredak na tablici rezultata.

7.2. Hackultet

Održan je drugi Hackultet, CTF natjecanje iz područja kibernetičke sigurnosti za studente. Natjecanje je provedeno u sklopu projekta e-Sveučilišta s ciljem promocije različitih područja kibernetičke sigurnosti i poticanja studenata na stvaranje karijere i jačanje stručnosti u tom

području. U zabavnoj i natjecateljskoj atmosferi, studenti su imali priliku testirati svoje znanje iz područja kao što su ranjivost weba, reverzni inženjering, binary exploitation i dr. U natjecanju je sudjelovalo 80 studenata/ica u 16 timova, a zastavice su osvajali punih 48 sati. Pobijedio je tim **Konsenzus** s 9605 bodova. Prva tri tima pozvana su na sudjelovanje u trenažnom kampu (eng. bootcamp) koji je ujedno i prilika za kvalifikaciju u nacionalni tim za European Cyber Security Challengeu (ECSC).

7.2.1. Trenažni kamp

Od 25. do 29. kolovoza 2025., u prostorijama Fakulteta elektrotehnike i računarstva u Zagrebu (FER), održan je CTF trenažni kamp u sklopu Hackultet natjecanja i projekta e-Sveučilišta. Kamp je organiziran u suradnji CARNET-ovog Sektora – Nacionalnog CERT-a i FER-ovog Laboratorija za sustave i signale (LSS), a okupio je natjecatelje koji su svoje znanje već pokazali na našim CTF natjecanjima. Temeljni cilj kampa bila je priprema najtalentiranijih natjecatelja za sudjelovanje na European Cybersecurity Challengeu (ECSC). Sudionici su imali priliku učiti od vrhunskih stručnjaka i pet dana proći kroz razne teme vezane uz kibernetičku sigurnost kao što su kriptografija, sigurnost web aplikacija, *binary exploitation*, sigurnost mreža, sigurnost automobila te *attack and defense* demonstraciju.

7.3. European Cybersecurity Challenge

Hrvatski nacionalni tim sudjelovao je na European Cyber Security Challengeu (ECSC) održanom u Varšavi od 6. do 9. listopada. ECSC je godišnje europsko natjecanje koje okuplja mlade talente iz cijele Europe kako bi se zabavili i natjecali u područjima kibernetičke sigurnosti. Deset natjecatelja praćena trenerom i voditeljem tima iskušali su svoje vještine u CTF (*Jeopardy Style* i *Attack and Defense)* obliku natjecanja.

Hrvatski nacionalni tim CrOwOatia – ECSC Varšava

8. Projekti

Nacionalni CERT je sudjelovao u provedbi projekata sufinanciranih sredstvima Europske unije: Podrška primjeni digitalnih tehnologija u obrazovanju – BrAIn, Hrvatska kvantna komunikacijska infrastruktura – CroQCI i projekt e-Sveučilišta.

8.1. Podrška primjeni digitalnih tehnologija u obrazovanju – BrAIn

Projekt BrAIn odnosi se na podršku u primjeni digitalnih tehnologija u obrazovanju, a u sklopu projekta koji se sastoji od šest elemenata, Nacionalni CERT nositelj je elementa 4 – Pametna kibernetička sigurnost.

Elementi projekta:

1. Edukacija i istraživanje
2. Pametne preporuke
3. Mrežni aspekti umjetne inteligencije
4. Pametna kibernetička sigurnost
5. Upravljanje projektom i administracija
6. Vidljivost i diseminacija

Pametna kibernetička sigurnost obuhvaća aktivnosti: uporaba umjetne inteligencije za automatizaciju internih procesa automatizacije obrade kibernetičkih incidenata, usklađivanje procesa s europskom i nacionalnom regulativom te unapređivanje sustava za ranu detekciju ranjivosti mogućih incidenata kao i primjenu umjetne inteligencije u izradi programa za podizanje svijesti o kibernetičkoj sigurnosti.

8.2. Hrvatska kvantna komunikacijska infrastruktura - CroQCI

Republika Hrvatska prepoznala je važnost inicijative Europske kvantne komunikacijske infrastrukture (EuroQCI) te je 2019. godine potpisala Deklaraciju o europskoj kvantnoj komunikacijskoj infrastrukturi čime se obvezala na provedbu aktivnosti na izgradnji sigurne kvantne komunikacijske infrastrukture koja će obuhvatiti cijelu Europsku uniju. Kao prvi korak na tom putu, formiran je **CroQCI** konzorcij.

CroQCI konzorcij čine ključne istraživačke i znanstvene institucije, ustanove visokog obrazovanja, javne ustanove i javna poduzeća ovlaštena od strane Ministarstva znanosti i obrazovanja za razvoj nacionalne QCI mreže te pripremu i provedbu nacionalnog projekta Hrvatska kvantna komunikacijska infrastruktura – CroQCI.

Cilj projekta je implementacija eksperimentalnih kvantnih komunikacijskih sustava i mreže, nadopunjenih i integriranih s rasponom klasičnih sigurnih komunikacijskih tehnologija. To uključuje izgradnju i testiranje uređaja i sustava koji kombiniraju najbolje od kvantnih, postkvantnih klasičnih i kvantno unaprijeđenih rješenja. CroQCI će osigurati arhitekturu mreže i projektnih scenarija uporabe koji će omogućiti integraciju zemaljske infrastrukture s budućom svemirskom komponentom u potpuno funkcionalnu kvantnu komunikacijsku mrežu.

Nacionalni CERT je nositelj radnog paketa 5 koji se odnosi na upravljanje ključevima i primjenu studija slučajeva. Radni paket sastoji se od osam aktivnosti: definiranje sučelja za prihvat ključeva u sustav za upravljanje ključevima (*Key Management System*), implementacija sustava za upravljanje ključevima, definiranje i implementacija aplikacijskog sučelja za enkripciju za pojedini slučaj primjene, kripto agilnost, studija primjene 1 - Unaprjeđenje sigurnosti distribuirane pohrane, studija primjene 2 – Sinkronizacija atomskog sata, studija primjene 3 - Svemirski segment kvantne distribucije ključeva (*Quantum Key Distribution*) i studija primjene 4 – Isporuka izvještaja provjere ranjivosti.

8.3. e-Sveučilišta

CARNET provodi projekt e-Sveučilišta s ciljem digitalne preobrazbe visokog obrazovanja u Republici Hrvatskoj poboljšanjem digitalne nastavne infrastrukture, uvođenjem digitalnih nastavnih alata te osnaživanjem digitalnih kompetencija nastavnika za poučavanje u digitalnom okruženju. U ustanovama visokog obrazovanja izgradit će se i/ili nadograditi mrežna i/ili računalna infrastruktura. Ustanove će dobiti napredno upravljanje mrežom sa sigurnosnom komponentom, mogućnost korištenja naprednih mrežnih servisa s osiguranim kapacitetom i stabilnosti veze. Ustanove će dobiti i popratne servise i alate kao i digitalnu nastavnu opremu. Kroz sve segmente opremanja fokus će biti na sigurnosnoj komponenti.

Aktivnosti kibernetičke sigurnosti provlače se horizontalno kroz sve projektne aktivnosti/elemente: mrežno računalne infrastrukture, servisne, računalne i obrazovne. U okviru aktivnosti kibernetičke sigurnosti planirana je izrada metodologije i uputa kako sigurnije organizirati lokalnu mrežu ustanove, pristup informacijskom sustavu ustanove, upravljanje servisima i infrastrukturom i uspostavu sigurnosnog nadzora lokalne mreže ustanove. Za sve navedene aktivnosti u suradnji s odabranim visokim učilištima kreirat će se tzv. PoC (eng. *proof of concept*), dokaz koncepta, kao pokazni primjer svim drugim krajnjim korisnicima, kako navedenu aktivnost uspostaviti uz Upute i edukativne aktivnosti u vlastitoj instituciji. U sklopu aktivnosti/elementa izvršit će se sigurnosna testiranja svih aplikacija i servisa razvijenih kroz projekt te razviti predlošci sigurnosnih politika za ustanove iz visokog obrazovanja te upute/priručnik za donošenje i provođenje sigurnosne politike. Djelatnici Nacionalnog CERT-a bit će na raspolaganju ustanovama za savjetovanje prilikom donošenja i provođenja sigurnosne politike. U cilju dizanja kapaciteta ustanova na reakciju na kibernetičke incidente, izradit će se

priručnik s uputama za reakciju na najčešće incidente te upute za bolju zaštitu (*hardening*) sustava i aplikacija.

Projekt e-Sveučilišta produljen je do 30. lipnja 2026. godine.

9. O Nacionalnom CERT-u

Nacionalni CERT (CERT.hr) je Sektor Hrvatske akademske i istraživačke mreže – CARNET koji se bavi obradom kibernetičkih incidenata, podizanjem svijesti i edukacijom o kibernetičkoj sigurnosti građana Republike Hrvatske.

CERT.hr se bavi incidentom ako se jedna od strana u incidentu nalazi u Republici Hrvatskoj odnosno, ako je u .hr domeni ili u hrvatskom IP adresnom prostoru, osim državnih tijela, pravnih osoba s javnim ovlastima i jedinica lokalne i područne (regionalne) samouprave, koje su u nadležnosti Nacionalnog centra za kibernetičku sigurnosti (NCSC).

Osim toga, Nacionalni CERT je nadležni CSIRT za pet sektora na temelju novog Zakona o kibernetičkoj sigurnosti (NN 14/24). Radi se o sljedećim sektorima: bankarstvo, infrastruktura financijskog tržišta, digitalna infrastruktura (za Registar naziva vršne nacionalne internetske domene), istraživanje te sustav obrazovanja.

Nacionalni CERT također obavlja zadaće CSIRT-a za javne i privatne subjekte, uključujući građanstvo.

Povijest Nacionalnog CERT-a započela je osnivanjem CARNET *Computer Emergency Response Team* (CARNET CERT) 1996. godine kao nacionalnog središta za sigurnost računalnih mreža. Nacionalni CERT – nacionalno središte za računalnu sigurnost osnovan je 2007. godine sukladno Zakonu o informacijskoj sigurnosti (NN 79/2007 od 30. 7. 2007. godine; 5. poglavlje) kao nacionalno tijelo za prevenciju i zaštitu od računalnih ugroza sigurnosti javnih informacijskih sustava u Republici Hrvatskoj čiji je osnovni zadatak obrada kibernetičkih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj. Godine 2016. ova se dva CERT-a spajaju u jedinstveni Odjel za Nacionalni CERT.

Osnivanjem Nacionalnog CERT-a započinje sustavan rad na zaštiti korisnika interneta, a 2003. godine izrađeno je zajedničko internet sjedište za Abuse službe pružatelja internetskih usluga u Hrvatskoj. Usluga filtriranja sadržaja za više od pola milijuna učenika koji internetu pristupaju iz osnovnih i srednjih škola uvedena je 2008. godine, a 2012. godine u suradnji s Ministarstvom unutarnjih poslova i Tehničkim veleučilištem pokrenut je Centar za sigurniji internet. Podizanje razine svijesti javnosti nastavljeno je provedbom brojnih aktivnosti, od kojih je najpoznatija kampanja Veliki hrvatski naivci.

10. Mali pojmovnik kibernetičkih incidenata

Nacionalni CERT obrađuje incidente ako se jedna od strana uključenih u incident nalazi u .hr domeni ili u hrvatskom IP adresnom prostoru. U nastavku se nalazi kratak opis često susretanih pojmova iz kibernetičke sigurnosti.

Pojam	Kratki opis

Backdoor alati	Alati koji omogućuju drugom korisniku da se služi žrtvinim računalom dok je žrtva spojena na Internet, bez znanja žrtve.
Bot/Botnet	Zaraženo računalo/mreža zaraženih računala.
Brute-force napadi	Testiranje svih kombinacija slova, brojeva i posebnih znakova s ciljem otkrivanja zaporki.
C&C	Iz engleskog Command&Control servers. Upravljački poslužitelj za nadzor i upravljanje računalima koja su dio botneta. Također se koristi izraz C2 poslužitelj.
DoS	Napad uskraćivanja usluge.
Malver	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika.
Malver URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu.
Payload	Malver koji akter prijetnje namjerava isporučiti žrtvi. Na primjer, ako je kibernetički kriminalac poslao e-poruku sa zlonamjernom makronaredbom kao privitkom, a žrtva se zarazi *ransomwareom*, tada je *ransomware* korisni teret (a ne e-pošta ili dokument).
Phishing	Pokušaj navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala.
Phishing URL	Poveznica do lažne Internet stranice na kompromitiranom web sjedištu ili sjedištu registriranom u svrhu krađe povjerljivih podataka.
Poslovna prijevara	Napadi kod kojih napadač lažnim predstavljanjem pokušava steći ili stekne financijsku korist od ciljanog poslovnog korisnika. Jedan on najčešćih oblika ovakvih napada su tzv. „CEO fraud“ ili „BEC“ (*Business Email Compromise*).
Ransomware	Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.
Scam	Pokušaj navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte). Najpoznatiji oblik je „nigerian scam“ ili „419 fraud“.
Smishing	Phishing putem sms-a.
Sniffing	Sniffing podrazumijeva neovlašteno presretanje mrežnog prometa.
Spam	Neželjena elektronička poruka reklamnog sadržaja.
Spam URL	*Spam* sadržaj na kompromitiranom *web* sjedištu koji se distribuira kroz *spam* poruke.
Spyware	Vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole.
SQL injection napadi	Napad umetanjem SQL kôda koji iskorištava ranjivosti na sloju baze podataka.
Tailgating	Napad društvenog inženjeringa gdje neovlaštena osoba dobiva fizički pristup ograničenom području prateći nekoga s pravom pristupa.
Web defacement	Kompromitirano web sjedište s izmijenjenim izgledom i sadržajem web stranice.

Nacionalni CERT u brojkama

Broj ustanova koje koriste usluge elektroničkih certifikata	213
Broj pretplata na CERT CVE	>516
Broj registriranih botova	126 098
Obrađenih kibernetičkih incidenata	1513
Analiza prijavljenih sigurnosnih događaja u CARNET mreži	210
Provjera sigurnosti CARNET aplikacija, komponenata i usluga	30
Objavljene novosti	95
Provjera ranjivosti	144
Broj objavljenih upozorenja	14
Posjeta portalu www.cert.hr	323 417
Broj pratitelja na Facebook @CERT.hr	2423
PiXi broj pojedinačnih korisnika	328
PiXi broj institucija koje koriste platformu	120
Broj provjerenih URL-ova pomoću usluge CERT iffy	37 191

Gdje nas sigurno možete naći?

Ovisno o tome kako možemo pomoći:

- za opće informacije: 01 6661 650 ili ncert@cert.hr
- za prijavu kibernetičkih incidenata: incident@cert.hr
- za upite medija: press@carnet.hr

Sve ostale informacije o Nacionalnom CERT-u nalaze se na adresi www.cert.hr.