2024.

CERT.hr

GODIŠNJI IZVJEŠTAJ

CARNET

SADRŽAJ

Uvod

Tijekom 2024. 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 **pad od 9,95%** u broju obrađenih incidenata u 2024. uspoređujući s pokazateljima iz 2023. godine. Pad u broju obrađenih incidenata ne znači smanjenje stvarnog broja incidenata. Važno je naglasiti da se radi samo o incidentima za koje je Nacionalni CERT zaprimio prijavu (od strane korisnika, partnera ili automatizirano). Osim toga, jedan prijavljeni incident ne znači da se statistički radi o jednom incidentu, već se incidenti kreiraju temeljem izvorišne IP adrese odnosno izvora napada. Veći izazov za proces obrade i rješavanja incidenta čine nove vrste incidenata, nove metode napada i inovativni i kreativni načini prijevare korisnika koje primjećujemo tijekom godine.

Incidenti tipa *phishing* činili su čak 58% svih obrađenih incidenata, a u odnosu na 2023. godinu, u 2024. godini **povećao se broj registriranih zaraženih računala u Hrvatskoj**. Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2024. godine iznosi 189 255, što je **povećanje od 36,47% u odnosu na 2023. godinu**.

U prošloj godini usluga **PiXi platforme** postala je zakonom određena jedinstvena ulazna točka za obavještavanje o kibernetičkim prijetnjama i incidentima kao Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima. Prema novom zakonodavnom okviru započet je proces pripreme PiXi platforme za korisnike i obveznike.

Predstavljen je novi sustav **CERT iffy** za provjeru internetskih trgovina, pomoću kojeg građani jednostavno mogu provjeriti sumnjive internetske trgovine i tako spriječiti krađu svojih osobnih podataka i novca.

Nacionalni CERT je aktivno sudjelovao u radu međuresornih radnih skupina u procesima transpozicije europskih akata iz područja kibernetičke sigurnosti u nacionalno zakonodavstvo i njihove operacionalizacije u okviru nadležnosti obveznika zakona.

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 2024". Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri na vježbi. Održana je vježba "Cyber Europe 2024" u organizaciji Agencije Europske Unije za kibernetičku sigurnost – ENISA-e na kojoj su se provježbavale procedure i odgovori na kibernetičke napade na energetski sektor te se ojačavala međunarodna i nacionalna suradnja.

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 **peto nacionalno CTF natjecanje iz područja kibernetičke sigurnosti za srednjoškolce Hacknite** i prvo CTF natjecanje za studente – Hackultet. **Natjecanje Hackultet** provedeno je u sklopu projekta e-Sveučilišta, a za sve zainteresirane omogućen je pristup edukativnoj platformi Hackultet na kojoj svi mogu unaprijediti svoje znanje iz područja kibernetičke sigurnosti rješavajući dostupne CTF zadatke.

U 2024. godini Nacionalni CERT je provodio aktivnosti i sudjelovao u projektima: **e-Sveučilišta, BraAIn, CroQCI i ZoomIn4PinkHats**.

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

Povodom **Dana sigurnijeg interneta**, s 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 s 185 536 na 192 502. Objavljene su 132 novosti iz područja kibernetičke sigurnosti. Povećan je broj posjetitelja i pratitelja na društvenim mrežama Facebook @CERT.hr – 2345 pratitelja i X @HRCERT – 1509 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 2024. 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.

Nataša Glavor

Pomoćnica 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 2024. 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.

Proaktivne mjere u brojkama u 2024. godini

Novosti	132
Broj pretplata na CERT CVE	206
Broj provjera ranjivosti	119
Broj izdanih elektroničkih certifikata	4350

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 2024. godini zabilježeno je **1113 kibernetičkih incidenata**, što je blagi pad u odnosu na godinu prije.

Pad ukupnog broja incidenata ne znači nužno da je bilo manje kibernetičkih napada. Statistika pokazuje broj obrađenih incidenata u Nacionalnom CERT-u za koje je prijava pristigla od građana, putem brojnih suradnji s drugim timovima ili automatizirano. Osim toga, kibernetički incidenti se u sustavima za obradu incidenta bilježe prema izvoru napada, odnosno po IP adresi s koje je napad ostvaren. To je najviše izraženo kod velikih phishing kampanji, kod kojih primjerice zaprimimo više desetaka prijava građana, no kako se radi o jednoj kampanji ona se bilježi kao jedan incident. U 2024. godini primijetili smo brojne izmjene u vektorima napada. Tako su napadači, primjerice, puno aktivniji na društvenim mrežama, na aplikacijama za instant komunikaciju te putem telefonskih poziva. Budući da se u velikom broju ovakvih prijava ne radi o incidentima koje obrađuje Nacionalni CERT, takve prijave prosljeđujemo drugim nadležnim institucijama, primjerice MUP-u i HAKOM-u.

Vrlo je velik **porast investicijskih prijevara**. Nažalost, građani, a posebno oni starije životne dobi, osjećaju posljedice inflacije te se nadaju brzoj i lakoj zaradi. Toga su svjesni i napadači te na vrlo agresivan način nagovaraju korisnike na ulaganja na raznim investicijskim platformama koje se na kraju pokažu lažnima. Ovakva vrsta prijevare spada u kibernetički kriminalitet koji rješava policija.

Phishing i phishing URL i dalje ostaju na vrhu statistika s udjelom od **58%** svih incidenata. Ako se radi o velikim phishing kampanjama s istim vektorom napada, statistički se to prikazuje kao jedan incident dok u pozadini stoji veći broj prijava korisnika.

Najveća promjena u odnosu na 2023. godinu je u tipu incidenta **„sustav zaražen zlonamjernim kôdom“**. Velik broj malvera korisnici detektiraju na vrijeme i pošalju prijavu, a s obzirom na to da korisnici nisu preuzeli malvere na svoje uređaje takve prijave tretiramo kao phishing. Osim toga, kod zaraženih sustava uvelike ovisimo o prijavama međunarodnih partnera. Primjerice, u prethodnoj godini provedeno je nekoliko koordiniranih akcija međunarodnih tijela za provedbu zakona i agencija za borbu protiv kibernetičkog kriminaliteta u kojima su pronađeni brojni C2 poslužitelji. Takvim akcijama otkriva se **velik broj botneta**, a Nacionalni CERT obavještava korisnike zaraženih računala u Hrvatskoj.

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.

Prikaz incidenata po tipu u 2024. godini

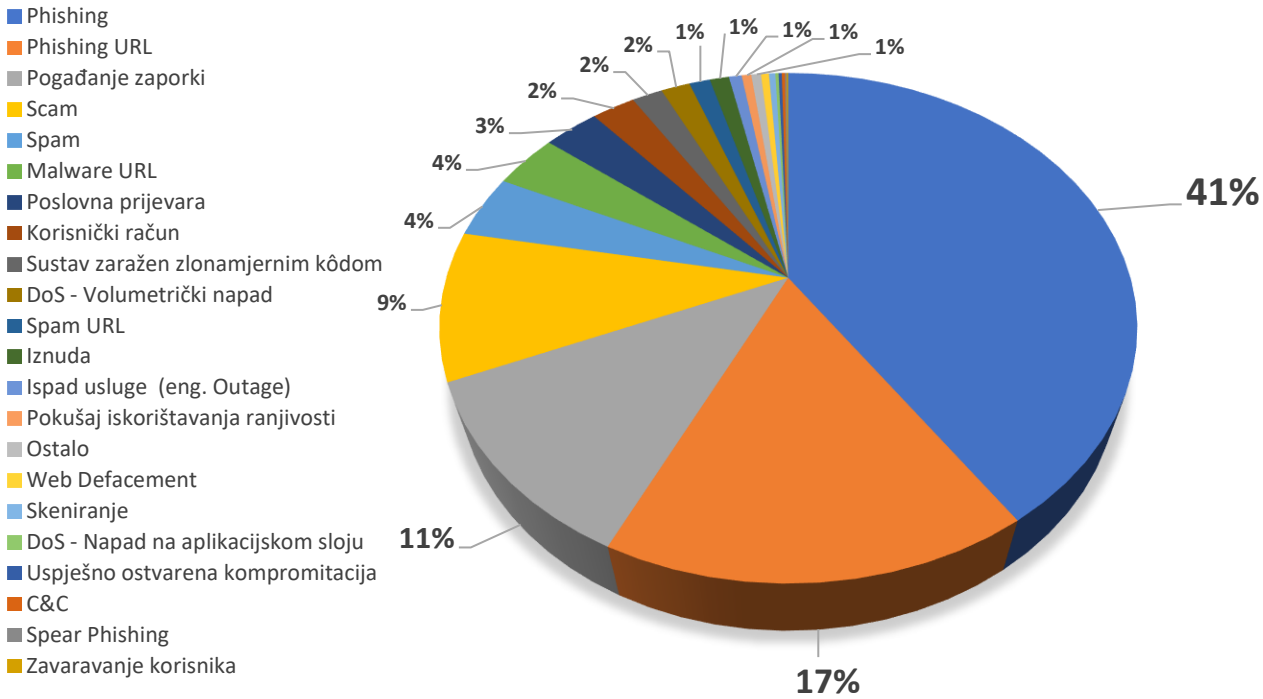
Phishing	451	▲
Phishing URL	185	▼
Pogađanje zaporki	127	▼
Scam	105	▼
Spam	45	▲
Malware URL	40	▲
Poslovna prijevara	34	▲
Korisnički račun	27	▲
Sustav zaražen zlonamjernim kôdom	19	▼
DoS - Volumetrički napad	18	▲
Spam URL	13	▼
Iznuda	12	▼
Ispad usluge (eng. Outage)	8	▲

Pokušaj iskorištavanja ranjivosti	6	▼
Ostalo	6	▲
Web Defacement	5	▼
Skeniranje	4	
DoS - Napad na aplikacijskom sloju	2	▲
Uspješno ostvarena kompromitacija	2	▲
C&C	2	
Spear Phishing	1	-
Zavaravanje korisnika	1	
UKUPNO	1113	▼

2.2. Raspodjela incidenata po tipu

Sljedeći grafikon prikazuje udjele incidenata po tipu u 2024. godini, koji su zabilježeni u sustavu za obradu incidenata.

Raspodjela incidenata po tipu u 2024. 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 2024. 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	99	78	74	90	120	86	104	68	90	86	94	124

Mjesečni prikaz broja obrađenih incidenata

Na grafičkom prikazu vidljiva su tri skoka u broju incidenata - u svibnju, prosincu te manji skok u srpnju.

Prvi skok u svibnju je zabilježen zbog povećanog broja **lažnih oglasa na društvenim mrežama**. Oglasi su sadržavali phishing poveznice te su se distribuirali putem društvenih mreža. Oglasi su imitirali poznate online trgovine te su često nudili lažne rasprodaje kako bi namamili žrtve te ostvarili novčanu korist. Također je zabilježen povećan broj prijava već dugo prisutnih **ucjenjivačkih poruka** eksplicitne tematike te "scam" poruka u kojima se napadači predstavljaju kao visokopozicionirani djelatnici MUP-a i u privitku šalju lažni sudski poziv ili sličan dokument.

Razlozi povećanog broja incidenata u srpnju su bile **phishing kampanje koje su ciljale korisnike banaka**. U e-mail porukama su se nalazile poveznice na stranice koje su nazivom i sadržajem imitirale sustav e-Građani te prijavu vjerodajnicama internet/mobilnog bankarstva hrvatskih banaka. Cilj kampanje je bila krađa pristupnih podataka za bankarske usluge. Također je zabilježen veći broj prijava phishing poruka koje su imitirale HZZO te u sebi sadržavale zlonamjernu datoteku.

Osim navedenog, nastavljene su i već spomenute scam poruke koje imitiraju djelatnika MUP-a.

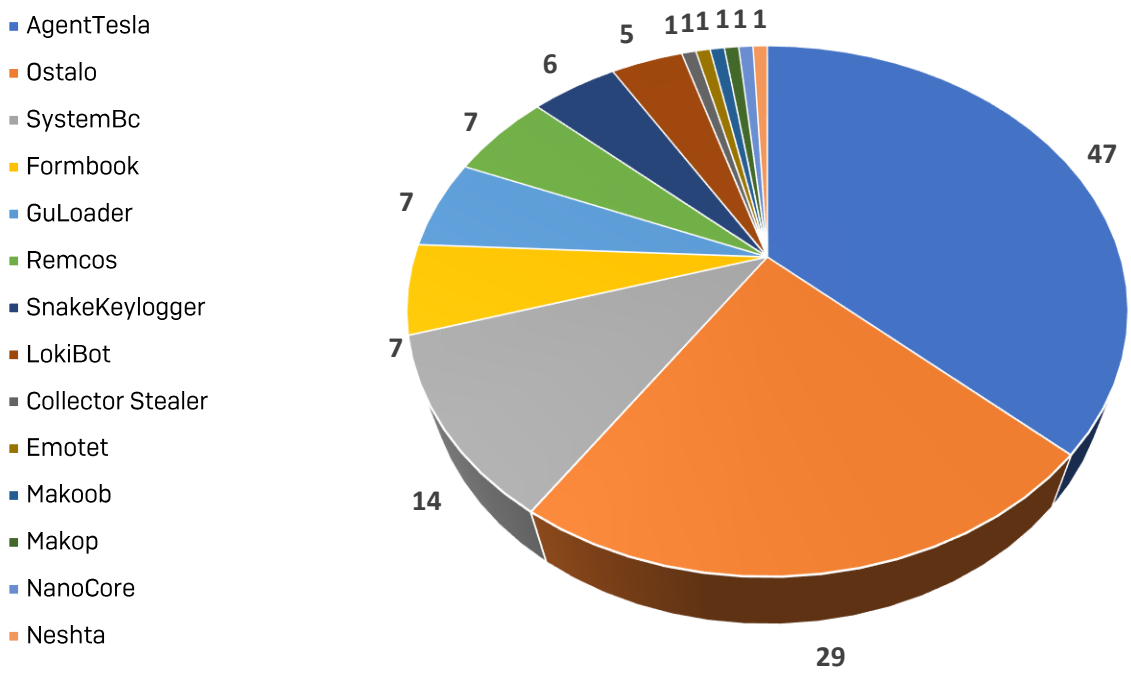
Povećan broj incidenata zabilježen je i u prosincu zbog **phishing i scam kampanja te lažnih oglasa na društvenim mrežama**. Od phishing kampanja vrijedi izdvojiti phishing poruke koje su imitirale poreznu upravu te sadržavale poveznice na phishing stranice kojima je cilj bio krađa osobnih podataka te podataka o bankovnim karticama. Lažni oglasi na društvenim mrežama su bili veoma slični kao već spomenuti, osim što su u ovom slučaju bile ponuđene lažne nagradne igre.

2.4. Vrste malvera

U 2024. godini otkriveno je 128 uređaja zaraženih malverom. Zaprimljeno je i analizirano 110 prijava 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
AgentTesla	47
Collector Stealer	1
Emotet	1
Formbook	7
GuLoader	7
LokiBot	5
Makoob	1
Makop	1
NanoCore	1
Neshta	1
Ostalo	29
Remcos	7
SnakeKeylogger	6
SystemBc	14



Prikaz malvera po tipu

Nacionalni CERT analizirao je 110 malvera, većinom distribuiranih putem elektroničke pošte. Većina malvera bila je "stealer" vrste. Vrste malvera poput nekih od AgentTesli, GuLoader malvera, LokiBota i sličnih obitelji često su u formatu NSIS installera što je alat za instaliranje softvera kojeg malver iskorištava kako bi uspostavio perzistenciju u legitimnim mapama na sustavu. Broj malvera koji koriste NSIS značajno je porastao te obuhvaća razne obitelji malvera, a eksfiltracija ukradenih podataka većinom se vrši putem Telegram ili Discord API sučelja. Velik broj malvera i dalje dolazi u .docx, .xls i sličnim ekstenzijama te lažnim "pdf" datotekama gdje je prava ekstenzija .exe s PDF ikonom.

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 hitne izmjene zaporki u slučaju kompromitacije. Navedeni malveri ciljaju zapamćene zaporke u preglednicima o čemu smo objavili dokument.

2.5. Registrirani botovi u Republici Hrvatskoj

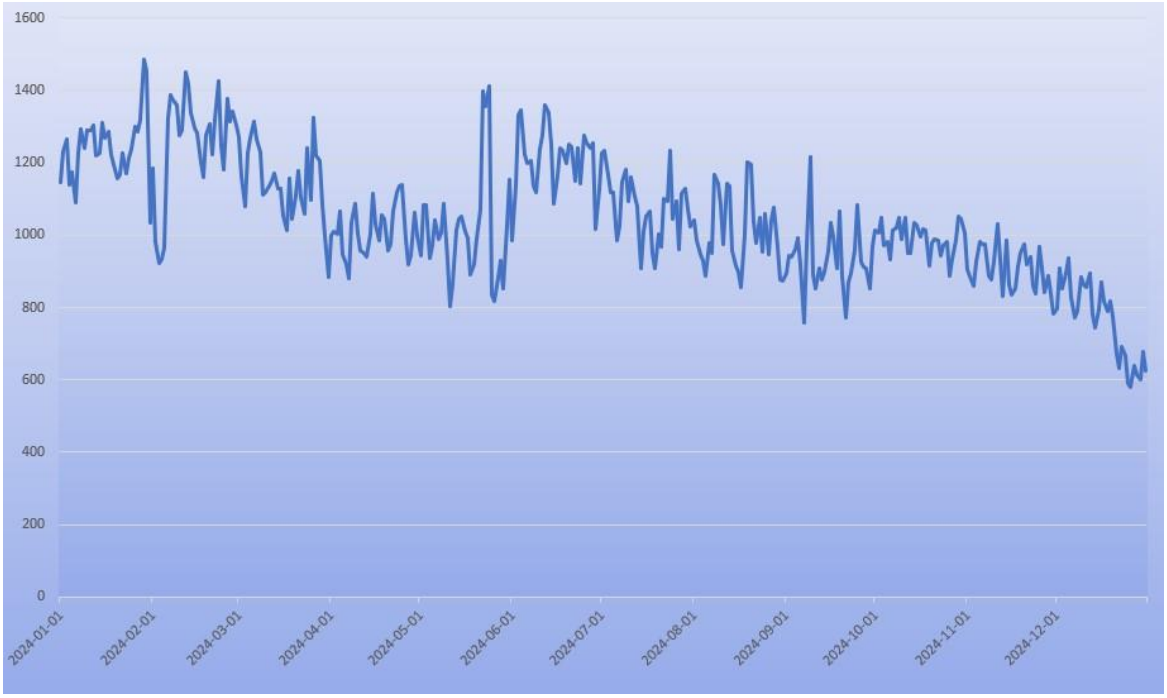
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani nadležnim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). U odnosu na 2023. godinu, u 2024. godini **povećao se broj registriranih zaraženih računala u Hrvatskoj**. Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2024. godine iznosi 189 255, što je **povećanje od 36,47% u odnosu na 2023. 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 2024. godini, koji su bili proslijeđeni davateljima internetskih usluga.

Deset najčešće prijavljivanih *botova* u RH

socks5_systemz	**56043**
Andromeda	**27926**
Vipersoftx	**15706**
apk.hummer	**14380**
pseudo_manuscrypt	**11040**
911-socks5-proxy	**8028**
Adload	**7919**
Mirai	**5381**
Gamut	**4919**
Moobot	**4534**



Broj zabilježenih *botova* po danima u 2024. godini

Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću oko **1045 *botova* dnevno**, što je više od prošle godine. Srednja vrijednost broja *botova* po danu za 2023. godinu iznosila je 800 što je **povećanje za više od 30%**.

2.6. Statistika o obrađenim incidentima koji su prijavljeni službi CARNET Abuse

Služba CARNET Abuse bavi se incidentom ako je izvor incidenta korisnik CARNET mreže (ustanova članica ili korisnik AAI@EduHr elektroničkog identiteta). Tijekom 2024. godine, služba **CARNET Abuse obradila je ukupno 940 incidenata**. Broj incidenata se smanjio za gotovo 47% u odnosu na prošlogodišnjih 1747. S obzirom na to da se i ove godine većina incidenata (gotovo 72%) odnosi na **povredu autorskih prava** (distribucija datoteke putem BitTorrent protokola koja je zaštićena autorskim pravom), procjenjujemo da se broj incidenata ponovno smanjio zbog još veće popularizacije streaming servisa multimedijskog sadržaja (npr. Netflix, HBO Max i sl.) te povećanog korištenja VPN-a. 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 #251 incident #phishing #smishing #vishing #DomainNameScam #CERTiffy	**Obrađen je 251 kibernetički incident.** Početkom godine bile su aktualne phishing stranice na društvenim mrežama koje imitiraju poznate tvrtke i brendove, a nude besplatne proizvode ili nagradne igre. Cilj phishinga je krađa osobnih i bankovnih podataka. Zaprimljene su prijave phishing poruka s phishing .html privitkom koji imitira poznate online servise. Maliciozna .html datoteka pomoću skripte šalje unesene podatke na drugi URL. Nastavljaju se hibridne (phishing/smishing/vishing) kampanje koje ciljaju korisnike hrvatskih banaka. Prijavljene su phishing poruke s umetnutim phishing URL-om i registrirane phishing stranice koji imitiraju internet bankarstvo za poslovne i privatne korisnike. Napadačima je cilj krađa 2FA tokena/PIN-a/jednokratne zaporke, preuzimanje ovlasti nad računom i mobilnom aplikacijom te krađa podataka o bankovnim karticama. Pojavile su se i smishing kampanje koje ciljaju korisnike pošte i kurirskih službi, koje upućuju na phishing stranice na kojima se nalazi obrazac za krađu bankovnih i osobnih podataka. Nacionalni CERT je zamijetio nove pokušaje prijevare u kojima putem telefonskog poziva prevaranti imitiraju policiju te uvjeravaju građane da im je osobna iskaznica korištena u kriminalnim radnjama. Ovakav tip prijevare se koristi za krađu osobnih podataka, a potencijalno i krađu financijskih sredstava. Prikupljeni brojevi pozivatelja su proslijeđeni HAKOM-u, a objavljeno je i upozorenje. Zaprimljeno je više prijava „Domain Name Scam“ prijevara u kojima napadači imitiraju registrare i kontaktiraju legitimne vlasnike domena. Za ovakve tipove prijevara smo objavili upozorenje. Iz vanjskih izvora je zaprimljeno više prijava lažnih online trgovina koje ciljaju hrvatske korisnike, od kojih su se neke nalazile na .com.hr vršnoj domeni. Nakon prijave registraru, domene su deaktivirane

	svim lažnim trgovinama na .com.hr domenama, dok je većina ostalih trgovina i dalje aktivna, ali i uvrštena u bazu servisa CERTiffy koji je pušten u rad krajem ožujka.
#Makop	Zaprimljena je prijava o ransomware napadu na srednju školu gdje je vektor napada bio javno izložen RDP (eng. *remote desktop protocol*). Radilo se o Makop ransomwareu. Nacionalni CERT analizirao je incident, ponudio tehničku pomoć te je pružena savjetodavna pomoć, poslane su upute za postupanje kod *ransomware* napada te sprječavanje njegova ponovnog nastanka. Osim navedenog, korisnik je upućen na prijavu policiji s obzirom na to da ova vrsta incidenta, između ostalog, spada u kibernetički kriminalitet.
#Ivanti ranjivosti	Zaprimljeno je više prijava ucjenjivačkih poruka poslanih sa stranih kompromitiranih e-mail adresa. Adresa kripto novčanika je prijavljena, ali su primijećene i uplate na istu. Objavljeno je upozorenje. Zaprimljene su informacije o kritičnim ranjivostima Ivanti sustava pod oznakama CVE-2023-46805 i CVE-2024-21887, koje u slučaju ulančanog iskorištavanja neautentificiranom napadaču omogućuju izvršavanje proizvoljnih naredbi na uređaju. Nacionalni CERT je poslao obavijest korisnicima te objavio upozorenje.
#Jenkins ranjivosti	Objavljeno je i upozorenje o kritičnim ranjivostima Jenkins poslužitelja pod oznakama CVE-2024-23897 i CVE-2024-23898, gdje su bile javno objavljene upute za iskorištavanje navedenih ranjivosti. Na taj način napadaču je omogućen pristup i čitanje proizvoljnih datoteka.
#Fortinet FortiOS ranjivosti	Poslane su obavijesti korisnicima Fortinet FortiOS sustava o kritičnim ranjivostima CVE-2024-21762 i CVE-2024-23113. Upozorenje o ranjivostima objavljeno je na mrežnim stranicama Nacionalnog CERT-a.

2. kvartal #296 incidenata #phishing porezna #vishing kriptovalute #phishing lažni oglasi #kompromitacija korisničkih računa #operacija Endgame	**Obrađeno je 296 kibernetičkih incidenata.** Zaprimljene su prijave o zlonamjernim web stranicama koje imitiraju Poreznu upravu te prijavu u NIAS, a vezane su uz temu povrata poreza. Cilj phishing stranica je krađa osobnih podataka i podataka o bankovnim karticama. Poslane su prijave izvorima incidenata te su stranice ugašene ubrzo nakon prijava. Nacionalni CERT bilježi nekoliko prijava korisnika u kojima ih napadači kontaktiraju telefonski ili putem maila zbog ulaganja u kriptovalute. Također, drugi obrazac pokušaja prijevare je kontakt potencijalne žrtve te povrat novca nakon kupovine kriptovaluta putem ilegalnih kripto mjenjačnica. U tom slučaju napadači obavještavaju žrtvu o isplativosti ulaganja te je potrebno da žrtva uplati određeni iznos kako bi joj se prethodno izgubljena sredstva isplatila na račun. Nacionalni CERT je objavio upozorenje. Primijećeno je više lažnih oglasa koji sadrže phishing poveznice, a distribuiraju se putem društvenih mreža. Oglasi imitiraju poznate online trgovine, te su napravljeni tako da zavaraju žrtve kako bi napadači ostvarili novčanu korist. Nacionalni CERT je izdao upozorenje za ovakav tip prijevara. Zaprimljene su prijave o lažnim oglasima koji sadrže phishing poveznice, a distribuiraju se putem društvene mreže. Takvi oglasi imitiraju ulaganja u poznate tvrtke iz energetskog sektora ili u kriptovalute. Vezano na ove prijetnje Nacionalni CERT prenio je obavijest Hrvatske udruge banaka na svojim mrežnim stranicama. Iz vanjskog izvora zaprimljena je prijava o kompromitiranim korisničkim računima prikupljenim tijekom operacije "Endgame". U navedenoj operaciji radilo se o suradnji više tijela ministarstava unutarnjih poslova, Europola i Eurojusta, koji su se uspješno infiltrirali u niz botneta. Na taj način prikupljeni su podaci o kompromitiranim računima koji su nam proslijeđeni. Poslane su obavijesti svim nadležnim kontaktima u vezi kompromitacije računa. Servisi iz financijskog sektora i sektora infrastrukture financijskog tržišta našli su se na popisu DDoSia projekta

#DDoSia projekt	(haktivistička grupa koja najavljuje i provodi DDoS napade). Informacija je proslijeđena financijskom sektoru iz NCERT nadležnosti, te GovCERT-u za tijela javne vlasti. Većina napada bila je uspješno zaustavljena, a za ostale se radilo o kratkotrajnom prekidu koji nije prouzročio veće posljedice.
#CEO fraud	Primijećen je povećan broj pokušaja CEO fraud prijevara na privatne tvrtke i obrazovne ustanove, što je rezultiralo većim brojem prijava incidenata u svibnju.
#scam	Nastavljene su scam kampanje gdje se imitiraju policijski službenici koji traže odgovor na priloženi sudski poziv ili tužbu. Objavljeno je i novo upozorenje na stranicama Nacionalnog CERT-a.
#Palo Alto PA-OS ranjivost	Poslane su obavijesti za Palo Alto PAN-OS ranjivost vlasnicima sustava. Radilo se o kritičnoj ranjivosti CVE-2024-3400 koja potencijalno omogućuje udaljenom, neautentificiranom napadaču izvršavanje proizvoljnog programskog kôda (RCE). O ranjivosti je objavljeno upozorenje na stranicama Nacionalnog CERT-a.
#Cisco ASA ranjivosti	Detektirane su dvije ranjivosti na Cisco ASA (*Adaptive Security Appliance*) i FTD (*Firepower Threat Defense*) softveru. Radi se o ranjivostima CVE-2024-20353 i CVE-2024-20359, koje napadačima omogućavaju izvršavanje proizvoljnog kôda i mogu dovesti do napada uskraćivanja usluge.
#Check Point sustavi ranjivost	Poslane su obavijesti za potencijalno ranjive Check Point sustave. Radilo se o CVE-2024-24919 ranjivosti koja napadaču potencijalno omogućuje čitanje osjetljivih informacija.

3. kvartal	Obrađena su 262 kibernetička incidenta.
#262 incidenta #phishing	Aktualne su i phishing kampanje koje ciljaju korisnike banaka. Radi se o domenama koje nazivom i sadržajem imitiraju sustav e-Građani te prijavu vjerodajnicama internet/mobilnog bankarstva hrvatskih banaka. Cilj je krađa podataka za pristup bankarskim uslugama. Zbog većeg broja prijava navedenih kampanji bilježimo skok broja prijavljenih incidenata u srpnju.
#Formbook malware	Zaprimljene su prijave za phishing poruke koje sadrže maliciozni privitak – Formbook malware. Izvor phishinga imitira HZZO u kontekstu potvrde o prijavi na obavezno zdravstveno osiguranje. Poslane su prijave izvorima incidenta i objavljeno je upozorenje.
#vishing	Primijećen je povećan broj vishing prijevara sa stranih brojeva gdje se napadači predstavljaju kao korisnička služba Microsofta ili drugih većih tvrtki, s ciljem krađe osobnih ili bankovnih podataka te novčanih sredstava. Korisnici su upućeni HAKOM-u i poslane su upute za prepoznavanje takvih prijevara.
#smishing	Aktualne su bile smishing prijevare u kojima se napadači predstavljaju kao dijete u nevolji koje se javlja roditeljima, a cilj je krađa novčanih sredstava putem SMS-a ili WhatsApp-a. Izdano je upozorenje.
#CUPS sustav ranjivosti	Detektirane su kritične ranjivosti CUPS sustava - *Common UNIX Printing System* (CVE-2024-47076, CVE-2024-47175, CVE-2024-47176, CVE-2024-47177). CUPS je kôd otvorenog izvora koji omogućuje printanje na Linux/Unix i sličnim operacijskim sustavima. Navedene ranjivosti vezane su za bibiloteke CUPS sustava, te neautentificiranom napadaču potencijalno omogućuju izvršavanje proizvoljnog kôda. Nacionalni CERT je izdao upozorenje.

4. kvartal #304 incidenta #investicijske prijevare #lažne web trgovine #digital skimming #scam #phishing kurirske službe	**Obrađena su 304 kibernetička incidenta.** U četvrtom kvartalu su i dalje aktualne investicijske prijevare putem reklama na društvenim mrežama. Radi se o stranicama koje nude ulaganje/kupovinu kriptovaluta, NFT prijevare, lažne dobitke u kriptovalutama, „online" poslove i slično. Često se radi o lažiranju izjava javnih osoba, traži se unos kontakt podataka nakon čega slijedi socijalni inženjering. Prijavljene su i platforme za „vraćanje" novca izgubljenih u prijevarama. Ususret Crnom petku i Cyber ponedjeljku povećan je broj kibernetičkih incidenata povezanih s online kupovinom. Prijavljeno je nekoliko lažnih web trgovina, web trgovina na kojima se nalazi digital skimming alat te jedno neovlašteno skeniranje web trgovine. Izdano je priopćenje za medije s naglaskom na lažne trgovine i uslugu iffy.cert.hr. Zaprimljene su prijave phishing poruka koje imitiraju poreznu upravu i prijavu poreza. Phishing stranica služi za krađu osobnih podataka te podataka bankovnih kartica. Za navedeno je izdano upozorenje. Nastavljene su scam kampanje koje imitiraju policijske službenike koji traže odgovor na priloženi sudski poziv ili tužbu. Zbog povećanog broja prijava je objavljeno novo upozorenje. Nastavljaju se phishing kampanje koje ciljaju korisnike pošte i kurirskih službi te pokušaji CEO fraud prijevara prema tvrtkama i obrazovnim ustanovama.

4. Usluge CARNET-ovog Nacionalnog CERT-a

4.1. CERT SPAMBLOK

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu Nacionalni CERT nudi uslugu CERT SPAMBLOK koja predstavlja sustav DNSBL (eng. *Domain Name Server Blacklist*) ili RBL sustav (eng. *Real Time Blacklist*) i dostupna je široj javnosti kao dodatak (*plugin)* za poslužitelje e-pošte. Svrha CERT SPAMBLOK usluge 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 postavljen na poslužiteljima e-pošte i mjesečno stavlja na crnu listu u prosjeku **44** jedinstvenih IP adresa i **5** jedinstvenih domena, a broj korisničkih upita za pristigle poruke elektroničke pošte u mjesečnom prosjeku iznosi **1356,87**.

cert spamblok

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 protekloj godini ukupan broj korisnika usluge je **206**, a ukupan broj posjeta stranici je **13 968**.

cert cve

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

Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima - Platforma PiXi je usluga koja služi za pravovremeno obavještavanje o prijetnji kako bi se spriječio incident i ubrzao proces zaustavljanja i rješavanja incidenta. Platforma PiXi se koristi od 2021. godine i služi za prijave značajnih incidenata prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te osigurava postupanje i izvještavanje prema Smjernicama za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga.

Prema pokazateljima korištenja usluge u protekloj godini ukupan broj korisnika usluge je 294 iz 120 institucija.

U prošloj godini usluga PiXi platforme postala je zakonom određena jedinstvena ulazna točka za obavještavanje o kibernetičkim prijetnjama i incidentima kao Nacionalna platforma za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima prema članku 43. Zakona o kibernetičkoj sigurnosti (NN 14/2024), Poglavlju IV. Uredbe o kibernetičkoj sigurnosti (NN 135/2024) i članku 15. Zakona o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor (NN 136/2024). Prema novom zakonodavnom okviru započet je proces pripreme PiXi platforme za korisnike i obveznike.

PiXi

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 2024. godini servis je koristilo više od 20 000 korisnika, a provjereno je čak 19 648 URL-ova. 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 2024. 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;

Tijekom 2024. godine Nacionalni CERT je u sklopu tih aktivnosti:

- 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 46 ustanova iz sustava obrazovanja, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže. U 2024. godini provedeno je ukupno 119 provjera 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 tvrtka Sectigo Limited 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 2024. godini izdano je ukupno 4001 SSL elektroničkih certifikata te 349 klijentskih elektroničkih certifikata. U studenom je uočen porast broj izdanih elektroničkih certifikata zbog obavijesti korisnicima o prekidanju rada sa Sectigo Limited tvrtkom. Već broj korisnika odlučio je obnoviti certifikate ranije kako ne bi morali navedeno činiti u prijelaznom razdoblju s jednog izdavatelja na drugog.

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 Europe 2024

U lipnju 2024. godine održana je sedma po redu paneuropska kibernetička vježba Cyber Europe. Vježba se održava u organizaciji ENISA-e, Agencije europske unije za kibernetičku sigurnost. Nacionalni CERT imao je ulogu igrača ali i nacionalnog koordinatora vježbe. Ciljevi vježbe su testiranje pripravnosti i jačanje sposobnosti EU na odgovor na kibernetičke incidente velikih razmjera i kibernetičkih kriza, gradnja povjerenja diljem EU ekosustava kibernetičke sigurnosti te omogućiti sudionicima mogućnost provježbavanja koja je jedinstvena s obzirom na intenzitet, značaj i pritisak generiran simulacijom kibernetičke krize.

U vježbi je simuliran koordinirani kibernetički napad na kritičnu infrastrukturu s naglaskom na energetski sektor. CARNET-ov Nacionalni CERT, kao nacionalni

koordinator vježbe, okupio je ukupno 78 kibernetičkih stručnjaka iz raznih tvrtki i institucija (SPAN, APIS-IT, KING-ICT, HAKOM, Hrvatski telekom, A1 Hrvatska) kako bi testirali svoju spremnost i snalaženje u ulogama koje bi imali u slučaju stvarnog napada. Zahvaljujući Spanu i Span Centru kibernetičke sigurnosti čak 40 igrača se okupilo uživo na jednom mjestu, dok su ostali sudjelovali online.

Scenarij vježbe započeo je simuliranim napadom na sustave za upravljanje električnom mrežom i distribuciju plina. Napad je rezultirao prekidima u opskrbi energijom, što je dovelo do značajnih smetnji u svakodnevnom životu i poslovanju. Tijekom simulacije, napadači su koristili sofisticirane metode kako bi infiltrirali sustave i onesposobili ključne komponente infrastrukture.

Kako se vježba odvijala, posljedice napada su se proširile na sektore prometa i zdravstva što je uzrokovalo poteškoće u pružanju zdravstvenih usluga i prekide u obavljanju prometnih usluga. Ovaj dio vježbe istaknuo je utjecaj poremećaja rada energetskog sektora na druge kritične usluge, pokazujući kako kibernetički napadi na jedan sektor mogu imati domino efekt na druge sustave i ljudski život.

Vježbe poput ove predstavljaju važan korak u jačanju otpornosti Europske unije na kibernetičke prijetnje, osiguravajući bolju zaštitu kritične infrastrukture i sigurnost građana. Više informacija o vježbi ali i atmosferi koja je vladala za vrijeme vježbe možete pronaći na našim stranicama.

CYBER EUROPE 2024
POWERED BY ENISA

5.2. Vježba Cyber Coalition 2024

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 24". 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. Organizirana je od strane Savezničkog zapovjedništva za transformacije (ACT), a održavala se od 30. studenoga do 6. prosinca 2024. na više desetaka lokacija u zemljama sudionicama. Vježba je okupila oko 1000 sudionika iz više od 30 zemalja.

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

CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u tehničkom dijelu, pravnom scenariju i kriznoj komunikaciji te su koordinirali sudjelovanje igrača i igračica iz privatnog sektora i akademske zajednice. 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. Na listi sudionika vježbe Cyber Coalition 24 su i tvrtke i institucije:

Iz privatnog sektora u vježbi su sudjelovale tvrtke: A1 Hrvatska d.o.o., Combis d.o.o., Utilis d.o.o., Končar Digital d.o.o., APIS IT d.o.o., Span d.d., HEP d.d., CS Computer Systems d.o.o., Infobip d.o.o., Offset Concepts, obrt za programiranje, CyberArrange Security Solutions j.d.o.o., Diverto d.o.o., Hrvatski Telekom d.d.

Iz akademske zajednice sudjelovali su: Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Fakultet prometnih znanosti Zagreb, Pravni fakultet Osijek, Pravni fakultet Zagreb i Visoko učilište Algebra. Vježbom se

rukovodilo iz NATO-vog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

5.3. 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.

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

6.1. Sporazum o poslovnoj suradnji s MUP-om

U 2024. 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 2024. godine provedeno je CTF natjecanje iz područja kibernetičke sigurnosti za srednje škole - Hacknite. Za potrebe natjecanja razvijeni su vrlo zanimljivi i izazovni sadržaji. Natjecanje i platforma Hacknite, na kojoj se nalaze zadaci i edukativni materijali, pružaju priliku svim zainteresiranim učenicima za učenje o kibernetičkoj sigurnosti. Više o samom natjecanju i platformi u poglavlju 7.1.

6.3. Zakon i Uredba o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga

Tijekom 2024. godine Zavod za sigurnost informacijskih sustava i Nacionalni CERT nastavili su s obavezama koje im kao nadležnim CSIRT-ovima proizlaze iz Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. Istim je Zakonom Nacionalni CERT proglašen nadležnim CSIRT-om za sve operatore ključnih usluga iz sektora bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, poslovnih usluga za državna tijela te davatelja digitalnih usluga. Osim toga, CARNET u Zakonu ima ulogu samog operatora ključne usluge (DNS usluga) kao i ulogu Tehničkog tijela za ocjenu sukladnosti.

6.4. 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 koji 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 obraditi Nacionalnom CERT-u kako bi zaprimale tjedne izvještaje o ranjivim servisima.

HRVATSKA UDRUGA BANAKA
CROATIAN BANKING ASSOCIATION

6.5. Obilježavanje Europskog mjeseca kibernetičke sigurnosti (ECSM)

CARNET-ov Nacionalni CERT kao nacionalni koordinator provedbe Europske kampanje "European Cyber Security Month" (ECSM) aktivno je obilježio Europski mjesec kibernetičke sigurnosti te su u listopadu provedene brojne aktivnosti s ciljem podizanja svijesti hrvatskih građana o kibernetičkoj sigurnosti. Događanja i materijali proteklih kampanja dostupni su na za preuzimanje i pregled na zajedničkoj stranici svih uključenih koordinatora https://cybersecuritymonth.eu/countries/croatia.

Tema prošlogodišnje kampanje bila je socijalni inženjering koji podrazumijeva manipulaciju žrtve kako bi se od nje ostvarila neka korist. U socijalni inženjering spada i phishing, a budući da u statistici naših obrađenih incidenata phishing čini 58% važno je građanima pojasniti ovu prijetnju i načine zaštite od nje.

U sklopu ECSM-a poruke su ciljanoj publici prenesene u obliku kratkih vide isječaka u kojima je prikazano na koji način napadači mog iskoristiti socijalni inženjering kako bi ostvarili svoj cilj. U GEANT-ovom serijalu prikazan je pokušaj socijalnog inženjeringa na sveučilištu s ciljem prikupljanja podataka o tajnom istraživanju, a u serijalu koji je snimio Nacionalni CERT prikazani su razni oblici *tailgatinga*, tehnike socijalnog inženjeringa s ciljem zaobilaženja sigurnosnih mehanizama za evidenciju i onemogućavanje ulaska neautoriziranim osobama u štićeni prostor.

Za vrijeme ECSM kampanje, provedeno je Hacknite natjecanje, a naš nacionalni tim sudjelovao je na European Cybersecurity Challenge natjecanju u Torinu. Objavljeni su brojni savjeti za prepoznavanje i zaštitu od socijalnog inženjeringa te su održana predavanja i webinari na teme kibernetičke sigurnosti. Zadnji dan ECSM-a predstavljeni su rezultati projekta ZoomIn4PinkHats o kojem možete više pročitati u poglavlju 8.4.

6.6. Dan sigurnijeg interneta 2024.

Dan sigurnijeg interneta obilježili smo jednom konferencijom i dva školska predavanja.

Na poziv OŠ Jure Kaštelana iz Zagreba i SŠ Ban Josip Jelačić iz Zaprešića održali smo predavanja na temu kibernetičke sigurnosti. U obje škole dočekali su nas učenici spremni naučiti nešto novo, razmijeniti vlastita online iskustva i postaviti pitanja o pravilnom postupanju prilikom dobivanja sumnjivih poziva ili sadržaja. Zahvaljujemo nastavnicima, profesorima, ravnateljima i stručnom osoblju obje škole što su prepoznali ovu temu i omogućili nam susrete uživo s učenicima željnima novih znanja iz područja kibernetičke sigurnosti.

U suradnji s udrugom Suradnici u učenju i Hrvatskom agencijom za mrežne djelatnosti – HAKOM-om održali smo na Dan sigurnijeg interneta tematsku konferenciju "Potraga za boljim internetom", s koje je poslana poruka o potrebi snažnije prevencije elektroničkog nasilja, zaštite osobnih podataka djece, stvaranja sigurnog virtualnog okružja te dostupnosti kvalitetnih internetskih sadržaja za djecu i mlade. Jedan od najvažnijih dana u kalendaru internetske sigurnosti okupio je brojne relevantne sugovornike, ali i nastavnike i učenike obrazovnih ustanova diljem Hrvatske kako bi se ukazalo na svakodnevnu potrebu zaštite djece i mladih.

Potraga za boljim internetom – okrugli stol

6.7. ConCERT

U 2024. održana je prva ConCERT konferencija na temu kibernetičke sigurnosti u organizaciji CARNET-ovog Nacionalnog CERT-a i Fakulteta elektrotehnike i računarstva (FER). Konferencija je okupila dvjestotinjak stručnjaka iz područja kibernetičke sigurnosti i studenata. Konferenciji je prisustvovao i ministar pravosuđa i uprave Ivan Malenica, koji je na otvaranju istaknuo kako Vlada i resorna ministarstva prepoznaju važnost kibernetičke sigurnosti i ulažu u obrazovanje djelatnika u ovome segmentu. Dekan Fakulteta elektrotehnike i računarstva prof. dr. sc. Vedran Bilas osvrnuo se na napore koje FER ulaže u obrazovanje budućih stručnjaka i uvrštavanje kibernetičke sigurnosti u kolegije koji se na FER-u podučavaju, a ravnatelj CARNET-a Hrvoje Puljiz naglasio je kako je razmjena informacija jedan od ključnih aspekata suradnje među svim sektorima, pogotovo o kibernetičkim prijetnjama. Dodao je kako se detalji kibernetičkih incidenata trebaju proširiti unutar zajednice kako bi različiti dionici zajednički radili na otkrivanju novih prijetnji. Na konferenciji se govorilo o dobrovoljnim mehanizmima zaštite (SK@UT), predstavljeno je Nacionalno koordinacijsko središte za industriju, tehnologiju i istraživanje u području kibernetičke sigurnosti (NKS), govorilo se o trenutnom stanju kibernetičke sigurnosti, izazovima koje predstavlja manjak stručnog kadra, o potrebi stalne obuke i drugim temama. Više o konferenciji pročitajte na našem portalu.

6.8. Djelovanje putem javnih medija i obraćanja javnosti

Djelovanje putem javnih medija

Nacionalni CERT je tijekom 2024. godine zaprimio brojne medijske upite za koje su pripremljeni informativni članci o temama poput lažnih web trgovina, internetskih prijevara, investicijskih prijevara, zlonamjernim softverima, Europskom mjesecu kibernetičke sigurnosti, projektima i djelovanju Nacionalnog CERT-a. Uz pisane medije, zabilježena su brojna gostovanja u televizijskim i radio emisijama posvećena temama iz kibernetičke sigurnosti. Velik interes medija zamijećen je u praćenju tema iz područja razvoja i primjene umjetne inteligencije te naše nove usluge CERT iffy.

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, 1st Cybersecurity Awareness

Raising konferenciju u organizaciji ENISA-e u Ljubljani, ConCERT konferenciju, sudjelovanje na konferenciji mreže FIRST u Japanu, CUC konferenciju, NKS konferenciju, Debug te BSides konferencije.

Nacionalni CERT je tijekom 2024. godine održao brojna predavanja za različite ciljne skupine od kojih bismo izdvojili radionicu "Kako kreirati učinkovitu kampanju za podizanje svijesti o kibernetičkoj sigurnosti", edukacije o sigurnosnim politikama i edukacije o elektroničkim certifikatima, trenažne kampove za ECSC nacionalni tim, učiteljice u sklopu ZI4PH projekta te trenažni kamp za sistemce visokih učilišta u sklopu projekta e-Sveučilišta.

Informirali smo javnost putem web sjedišta Nacionalnog CERT-a (https://www.cert.hr/) kojeg je 2024. godine posjetilo ukupno 192.502 posjetitelja te putem društvenih mreža Facebook (2345 pratitelja) i Twitter (1509 pratitelja).

7. CTF natjecanja

7.1. HACKNITE 2024

Peto izdanje hrvatskog CTF natjecanja za srednjoškolce HACKNITE provedeno je od 18. do 20. listopada 2024. 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 380 učenika u 76 srednjoškolska tima iz 32 srednje škole. Pobjednički tim bio je tim **taqi** sastavljen od učenika XV. gimnazije, Gimnazije Andrije Mohorovičića Rijeka i Tehničke škole Ruđera Boškovića Zagreb.

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 prvi 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 90 studenata/ica u 18 timova, a zastavice su osvajali punih 48 sati. Pobijedio je tim **/dev/null** s maksimalnih 6000 bodova riješivši svih 40 zadataka. 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 26. do 30. kolovoza 2024., 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 25 studenata 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.

Trenažni kamp

7.3. European Cybersecurity Challenge

Hrvatski nacionalni tim CrOwOatia, sudjelovao je na European Cyber Security Challenge-u (ECSC) održanom u Torinu od 7. do 11. 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-u (*Jeopardy Style* i *Attack and Defense)* obliku natjecanja.

Hrvatski nacionalni tim CrOwOatia – ECSC Torino

8. Projekti

Nacionalni CERT je sudjelovao u provedbi četiri projekta sufinancirana sredstvima Europske unije: Podrška primjeni digitalnih tehnologija u obrazovanju – BrAIn, Hrvatska kvantna komunikacijska infrastruktura – CroQCI, e-Sveučilišta i ZoomIn4PinkHats – ZI4PH.

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. Projekt traje od ožujka 2022. do prosinca 2025. godine. 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.

8.4. ZoomIn4PinkHats

Sektor - Nacionalni CERT uspješno je proveo projekt pod nazivom "ZoomIn4PinkHats – ZI4PH". Projekt je financiran kroz GÉANT *Innovation Programme* 2024. Cilj projekta bio je **promicanje vještina kibernetičke sigurnosti** među ženama zaposlenim u obrazovanju, odnosno osnaživanje nastavnica kako bi provodile aktivnosti vezane uz kibernetičku sigurnost među učenicima, educirajući ih kroz radionice o različitim temama kibernetičke sigurnosti i potičući stvaranje zajednice učenja i razmjene znanja i vještina.

U sklopu projekta održan je trenažni kamp (*bootcamp*) za profesorice, nastavnice i mentorice iz 14 srednjih i osnovnih škola. Polaznice treninga stigle su iz 12 gradova: Dubrovnika, Splita, Makarske, Osijeka, Pule, Zadra, Rijeke, Samobora, Zaprešića, Ivanić Grada, Velike Gorice i Zagreba. Održanim treningom osnažili smo i educirali polaznice zaposlene u srednjim i osnovnim školama za provedbu daljnjih aktivnosti edukacije učenica i pružanje podrške u njihovim projektima i radionicama koje provode s ciljem učenja o različitim temama kibernetičke sigurnosti i popularizacije područja kibernetičke sigurnosti među učenicama.

Završna konferencija projekta održana je u hotelu International u Zagrebu, a osim učiteljica koje su sudjelovale u projektu i njihovih učenica, konferencija je okupila i istaknute stručnjakinje iz raznih sektora, uključujući predstavnice Ministarstva vanjskih i europskih poslova, A1 Hrvatska, Algebre, Nacionalnog CERT-a, Ministarstva unutarnjih poslova, Hrvatskog katoličkog sveučilišta te ureda Pravobraniteljice za ravnopravnost spolova.

Rezultati projekta su vidljivi već u 2024. godini jer se broj učenica među natjecateljima Hacknite natjecanja povećao za 10% u odnosu na 2023. godinu.

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 tijela državne uprave za koje je do transpozicije NIS2 Direktive bio nadležan Zavod za sigurnost informacijskih sustava (ZSIS).

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.

Gdje nas sigurno možete naći?

Ovisno o tome kako možemo pomoći;

- za opće informacije nazovite na 01 6661 650 ili pišite na ncert@cert.hr

- kibernetičke incidente prijavite na incident@cert.hr

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

Nacionalni CERT u brojkama	
Poslužiteljski elektronički certifikati	4001
Klijentski elektronički certifikati	349
Broj pretplata na CERT CVE	206
Broj registriranih botova	189 255
Obrađenih sigurnosnih incidenata	1113

Analiza prijavljenih sigurnosnih događaja u CARNET mreži	100
Provjera sigurnosti CARNET aplikacija, komponenata i usluga	11
Objavljene novosti	132
Provjera ranjivosti	119
Broj objavljenih upozorenja	12
Posjeta portalu www.cert.hr	192 502
Broj pratitelja na Facebook @CERT.hr	2345
Broj pratitelja na Twitter @HRCERT	1509
PiXi broj pojedinačnih korisnika	294
PiXi broj institucija koje koriste platformu	120
Broj provjerenih URL-ova pomoću usluge CERT iffy	19 648

KONTAKT

Josipa Marohnića 5, Zagreb, HR-10000
www.cert.hr
ncert@cert.hr (opće informacije)
incident@cert.hr (prijave incidenata)
press@carnet.hr (upiti medija)