GODIŠNJI IZVJEŠTAJ NACIONALNOG CERT-A ZA 2021. GODINU

CERT.hr
surfaj sigurnije

CARNET
znanje povezuje

SADRŽAJ

1. O NACIONALNOM CERT-U

Nacionalni CERT (**CERT.hr**) je odjel Hrvatske akademske i istraživačke mreže – **CARNET** osnovan sukladno **Zakonu o informacijskoj sigurnosti** (NN 79/2007 od 30.07.2007. 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 računalno-sigurnosnih incidenata s ciljem očuvanja kibernetičke sigurnosti u Republici Hrvatskoj.

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 nadležan **Zavod za sigurnost informacijskih sustava** (ZSIS). Osim toga, Nacionalni CERT se bavi incidentima sa znatnim učinkom prema **Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga** za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga.

Usluge CERT.hr-a dostupne su široj javnosti. Djelovanje CERT.hr-a dijelom je financirano sredstvima koja osigurava Ministarstvo znanosti i obrazovanja, a drugi dio Europska unija kroz razne EU projekte.

Tijekom 2021. godine Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih 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.

Neke od proaktivnih mjera koje provodi Nacionalni CERT su:

- **diseminacija informacija iz područja računalne sigurnosti** - izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- **praćenje računalno-sigurnosnih tehnologija** - 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;**
- **sigurnosna testiranja CARNET-ovih usluga i servisa te aplikacija koje pristupaju sustavu eMatica;**
- informiranje javnosti putem portala **www.antibot.hr** s ciljem pružanja pristupačnih i jednostavnih savjeta krajnjim korisnicima;
- **unapređenje svijesti o značaju računalne sigurnosti** - organiziranje i provedba aktivnosti podizanja svijesti o kibernetičkoj sigurnosti;
- **edukacija i obuka o računalnoj sigurnosti;**
- **održavanje predavanja i webinara o sigurnosti na internetu;**
- sudjelovanje u televizijskim i radijskim emisijama;
- sudjelovanje na predavanjima u sklopu konferencija i radionica.

ALATI	2
DOKUMENTI	3
NOVOSTI	128
BROJ PRETPLATA NA CERT EPSILONU	133
BROJ PROVJERA RANJIVOSTI	214
BROJ IZDANIH ELEKTRONIČKIH CERTIFIKATA	1634

Broj izvršenih proaktivnih mjera u 2021. godini

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. Neke od reaktivnih mjera koje provodi Nacionalni CERT su:

- **postupanje s računalno-sigurnosnim incidentima** - obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);
- **koordinacija rješavanja značajnijih incidenata** - obrada incidenata sa znatnim učinkom sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga;
- **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 RAČUNALNIH INCIDENATA I STATISTIKE

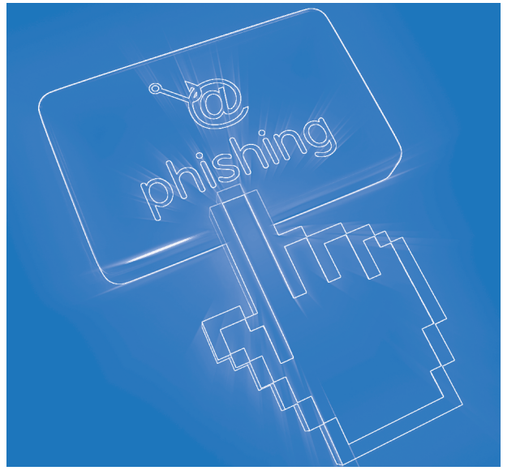
2.1. STATISTIKA O OBRAĐENIM INCIDENTIMA

Nacionalni CERT je tijekom 2021. godine zaprimio i obradio ukupno 1211 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su ***phishing URL, phishing i malware URL.***

Promjena u odnosu na prošlu godinu je manji broj korisničkih prijava računalno-sigurnosnih incidenata. Korištenjem OSINT metoda (eng. Open Source Inteligence) za otkrivanje računalno-sigurnosnih incidenata na web sjedištima pod nadležnošću Nacionalnog CERT-a, ali i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta, u odnosu na 2020. godinu Nacionalni CERT je zaprimio i obradio 29% incidenata manje.

Velika promjena odnosi se na rast broja incidenta koji su klasificirani kao *malware URL* koji je u 2021. godini ponovno nakon pet godina došao na 3. mjesto. Razlog tome su korištenje OSINT metoda i automatizirane prijave kompromitiranih sjedišta na kojima se nalaze zlonamjerne skripte.

S obzirom na to da ***web defacement, phishing URL, malware URL i spam URL*** zapravo predstavljaju kompromitirana web sjedišta, ako se gleda sumarno, broj otkrivenih kompromitiranih web sjedišta smanjio se za 23% u odnosu na prethodnu godinu.



TIP INCIDENTA	BROJ	TREND
PHISHING URL	353	–
PHISHING	166	–
MALWARE URL	139	▲
WEB DEFACEMENT	112	–
POGAĐANJE ZAPORKI	111	▼
SUSTAV ZARAŽEN ZLONAMJERNIM KODOM	96	▲
POKUŠAJ ISKORIŠTAVANJA RANJIVOSTI	57	▲
DOS - VOLUMETRIČKI NAPAD	39	▲
SCAM	25	–
KORISNIČKI RAČUN	20	▲
SPAM	20	▼
OSTALO	17	▲
PRIJEVARE	17	▲
HOAX	15	▼
DOS - NAPAD NA APLIKACIJSKOM SLOJU	11	▲
ISPAD USLUGE (ENG. OUTAGE)	6	▲
C&C	3	▼
SKENIRANJE	3	▼
PRIKUPLJANJE INFORMACIJA	1	▲
UKUPNO	**1211**	▼

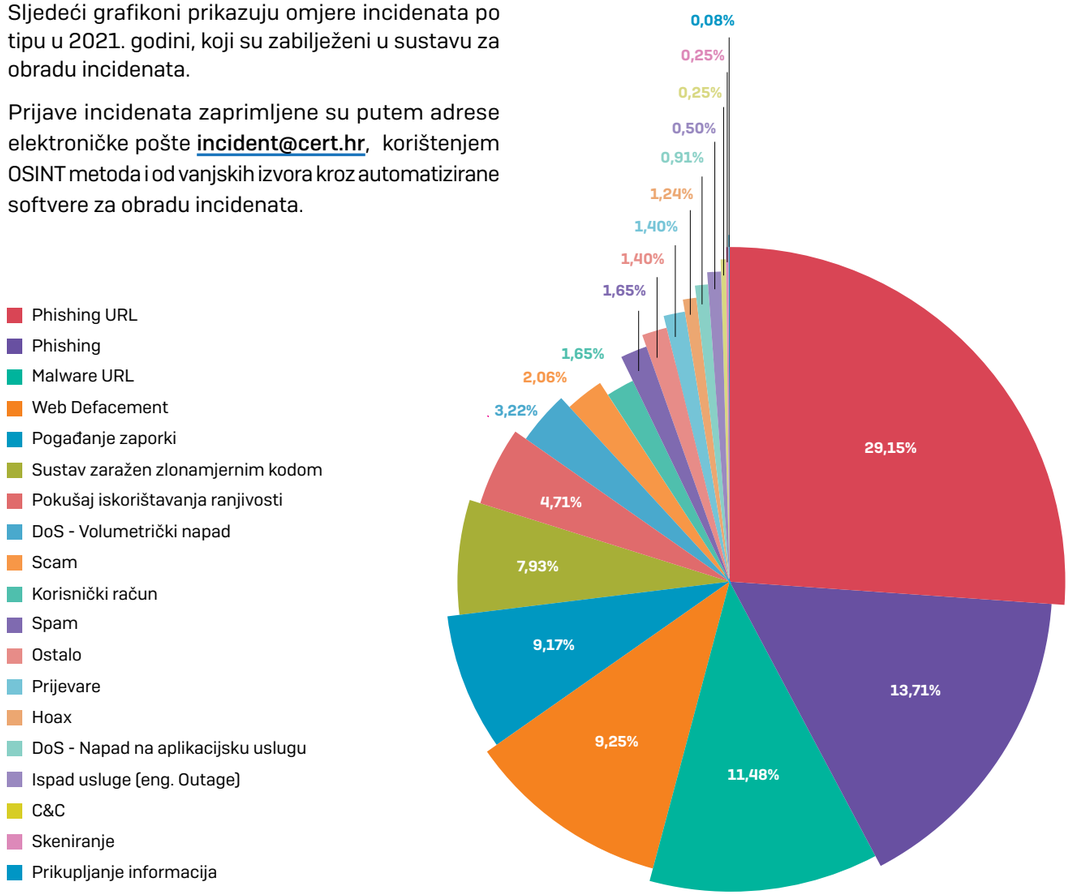
Prikaz incidenata po tipu u 2021. godini

Prema trendu kretanja vrsta incidenata vidimo da je većina kategorija incidenata u porastu, što je rezultat velikog broja prijava općenito (zbog povećanja suradnje i velikog broja aktivnosti vezanih uz vidljivost samog Nacionalnog CERT-a). Pad broja pojedinih kategorija je rezultat novih i sofisticiranih metoda napada koje se izvode kroz *phishing* prijevare i ostale tehnike socijalnog inženjeringa.

2.2. RASPODJELA INCIDENATA PO TIPU

Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2021. godini, koji su zabilježeni u sustavu za obradu incidenata.

Prijave incidenata zaprimljene su putem adrese elektroničke pošte **incident@cert.hr**, korištenjem OSINT metoda i od vanjskih izvora kroz automatizirane softvere za obradu incidenata.

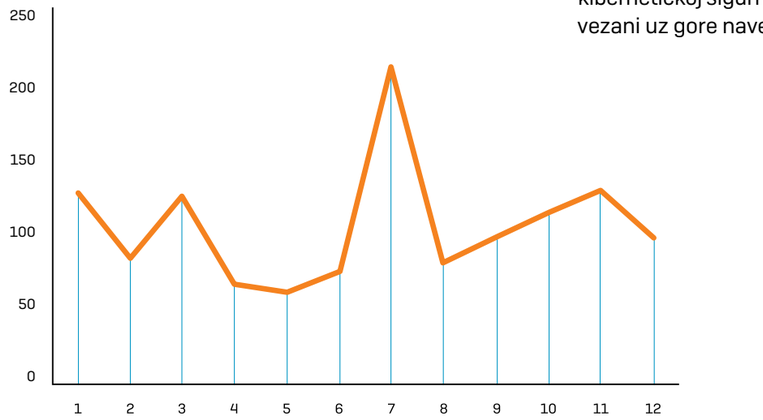


Raspodjela incidenata po tipu u 2021. godini

2.3. TRENDOVI POJAVA INCIDENATA NA POSLUŽITELJIMA U 2021. GODINI

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

Na grafičkom prikazu vidljiva su tri skoka u broju incidenata: u ožujku, srpnju i studenom. Prvi skok u ožujku zabilježen je radi povećanog broja incidenata vezanih uz ranjivosti **Microsoft Exchange** sustava i aplikacija za virtualizaciju VMWare vCenter. Nacionalni CERT je detektirao potencijalno kompromitirane poslužitelje te poslao prijave korisnicima s uputama za detaljnu provjeru sustava i preporukom za nadogradnju u kojoj su ranjivosti ispravljene.



1	2	3	4	5	6	7	8	9	10	11	12	MJESEC
132	77	131	58	56	68	219	71	91	107	126	75	BROJ INCIDENATA

Broj incidenata na poslužiteljima u 2021. godini po mjesecima

Razlog povećanja broja incidenata u srpnju je korištenje OSINT metoda kojima je otkriven veći broj zlonamjernih stranica i kompromitiranih web sjedišta s izmijenjenim izgledom i sadržajem web stranica. Nacionalni CERT je poslao prijave svim nadležnim pružateljima usluga udomljavanja Internet stranica.

Povećan broj incidenata bio je i u studenom kada su bile aktivne kampanje vezane uz online trgovinu, zbog nadolazećih blagdana te Crnog petka i Cyber ponedjeljka. Nacionalni CERT je zaprimio i obradio prijave incidenata koje se odnose na lažne nagradne igre, a OSINT metodama je pronašao i 60-ak lažnih online trgovina. Zbog unapređenja svijesti o kibernetičkoj sigurnosti, izdane su **upute i indikatori** vezani uz gore navedene vrste incidenata.

2.4. REGISTRIRANI BOTOVI U REPUBLICI HRVATSKOJ

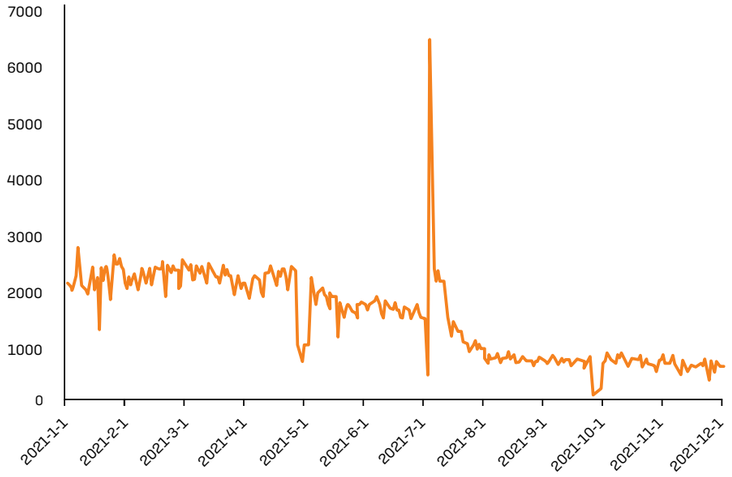
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani nadležnim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). Iz grafikona koji prikazuje godišnji trend broja *botova* vidljivo je da se u Hrvatskoj broj registriranih zaraženih računala neznatno smanjuje u odnosu na prethodnu 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 2021. godini, koji su bili proslijeđeni davateljima internetskih usluga

Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2021. godine iznosi 236 834, što je smanjenje od 62.6% u odnosu na 2020. godinu.

APK.HUMMER	72321
ANDROMEDA	48457
FLUBOT	32871
GAMUT	19637
CONFLICKER	12095
NECRUS	11656
MONERO	4375
MIRAI	4171
QSNATCH	4086
UNKNOWN	2636

Top 10 botova prema tipu u 2021. godini



Broj zabilježenih botova po danima u 2021. godini

Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću ispod 2000 *botova* dnevno, što je bio slučaj i prošle godine. Godišnji trend broja *botova* - Srednja vrijednost broja *botova* po danu za 2021. godinu iznosila je 1.393,76 što je smanjenje za nešto više od 300 *botova* u odnosu na 2020. godinu.

2.5. 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 2021. godine služba CARNET Abuse obradila je ukupno 5823 incidenta. Suradnjom s ostalim pružateljima internetskih usluga (eng. *Internet Service Provider* – ISP) u Hrvatskoj, dio incidenata obrađuje se kod davatelja usluge koju pojedini korisnik koristi. Gotovo 80% incidenata odnosi se na povredu autorskih prava (distribucija datoteke putem BitTorrent protokola koja je zaštićena autorskim pravom). Drugi najčešći incident je pokušaj neovlaštenog pristupa računalu i/ili mreži. U ostalim slučajevima, korisnike se najčešće upućuje na portal **antibot.hr** kako bi skenirali računalo i očistili ga od zlonamjernog sadržaja.

3. ZNAČAJNIJI INCIDENTI, OTKRIVENE RANJIVOSTI I DOGAĐAJI

1. KVARTAL

#340 incidenata #sextortion #phishing kampanje #Emotet

U prvom kvartalu 2021. godine obrađeno je **340** računalno-sigurnosnih incidenata. U **siječnju** je detektiran povećan broj lažnih ucjenjivačkih poruka kojima napadač pokušava iznuditi novčanu dobit od žrtve. Nacionalni CERT poslao je prijave davatelju usluga s čijeg su se poslužitelja distribuirale poruke. Dodatno, objavljeno je **upozorenje** na našim stranicama.

Zaprimljene su prijave o višestrukim pokušajima neovlaštenog skeniranja web servisa financijskih institucija te prijave *phishing* kampanja koje su putem lažnih formi za prijavu pokušale doći do korisničkih pristupnih podataka. Nacionalni CERT je poslao prijave nadležnim CERT-ovima i pružateljima digitalnih usluga kako bi se spriječili daljnji napadi i uklonile *phishing* stranice.

U zajedničkoj akciji policijskih snaga i vlasti Nizozemske, Njemačke, Sjedinjenih Američkih Država, Ujedinjenog Kraljevstva, Francuske, Litve, Kanade i Ukrajine, uz koordinaciju organizacija Europol i Eurojust, preuzeta je infrastruktura korištena za širenje zlonamjernog sadržaja **Emotet**. Od nizozemskih kolega zaprimili smo podatke o potencijalno kompromitiranim podacima prikupljenima ovom akcijom, a korisnicima čiji se podaci nalaze u dostavljenim bazama, a vezani su uz **.hr domenu** poslane su obavijesti o kompromitaciji uz savjete kako se zaštititi.

2. KVARTAL

#182 incident #Facebook leak #samouništenje Emoteta #phishing

U drugom kvartalu obrađena su ukupno **182** incidenta. Na jednom hakerskom forumu objavljeni su razni podaci više od 533 milijuna korisnika Facebooka iz 106 zemalja. Među objavljenim podacima mogli su se pronaći telefonski brojevi, imena i prezimena, lokacije, adrese e-pošte i drugi osobni podaci. O navedenom događaju Nacionalni CERT je informirao građane te im uputio sigurnosne preporuke kako postupati u slučaju ako su njihovi podaci postali javno dostupni. U **travnju** su europske policijske snage nakon više od tri mjeseca istrage uklonile zlonamjerni sadržaj Emotet sa svih zaraženih računala pomoću prilagođene DLL datoteke koja je aktivirana u nedjelju, 25. travnja i dovela do samouništenja Emoteta. Što se tiče hrvatskog IP adresnog prostora, skoro dvije tisuće jedinstvenih IP adresa komuniciralo je s preuzetom infrastrukturom zlonamjernog sadržaja Emotet, ali od travnja su sva računala postala *emotet-free*.

Jedan od hrvatskih pružatelja internet usluga prijavio je lažnu stranicu na kojoj su se nalazili osobni podaci korisnika od više hrvatskih pružatelja usluga. Nacionalni CERT poslao je prijavu stranom pružatelju usluga udomljavanja te je stranica ubrzo nakon prijave bila uklonjena.

U **lipnju** je detektiran povećan broj *phishing URL-ova* koji ciljaju korisnike internetske prodaje, a putem elektroničke pošte proširila se phishing kampanja u kojoj se napadač lažno predstavlja kao banka s ciljem ostvarivanja financijske koristi od žrtve. Na jezično neispravnom i pogrešnom hrvatskom jeziku korisnika se obavještava o navodnim sumnjivim pokušajima prijave na njihov bankovni račun te se od njih traži potvrda identiteta upisom imena i prezimena, broja kartice, datuma isteka kartice te sigurnosnog koda (CVV) kako ne bi "izgubili" svoj račun. Nakon unosa traženih podataka korisnika se preusmjerava na lažnu stranicu za unos bankovnog tokena. Nacionalni CERT poslao je više prijava izvorima napada (*hosting provideru*, stranom CERT-u, stranom SOC-u (*Security Operations Center*) te centru za suzbijanje *phishing* poruka), izdao upozorenje na službenim stranicama kao i preporuke kako prepoznati ovakve prijevare i od njih se zaštititi.

3. KVARTAL

#381 incident #smishing #All World Cards

U trećem kvartalu obrađen je ukupno **381** incident. **Srpanj** nam je donio povećan broj URL-ova zaraženih zlonamjernim softverom (*malware URL*), njih čak 73, a povećao se i broj slučajeva *phishing URL-ova*. Tijekom srpnja prijavljen je velik broj *phishing* prijevara koje su ciljale korisnike nekoliko hrvatskih banaka. *Phishing* prijevare distribuirale su se putem elektroničke pošte i sadržavale su *phishing* poveznice koje imitiraju usluge Internet bankarstva. Pojavila se i tzv. *Smishing* kampanja (*phishing* putem SMS-a) koja je putem zaraženih uređaja širila poveznicu na stranicu sa zlonamjernim sadržajem. Nacionalni CERT je izdao obavijest putem društvenih mreža te je poslao prijave pružateljima usluga udomljavanja na čijim su se mrežnim stranicama nalazili različiti stupnjevi zlonamjernog sadržaja.

U **kolovozu** je kroz suradnju s CSIRT Network zajednicom (zajednica europskih CERT timova), na uvid dobivena kolekcija *„All World Cards"*, koja je prikupljena iz više izvora, a sadrži milijun zapisa s brojevima kartica, CVV oznakom, datumom isteka kartice i osobnim podacima korisnika. Podaci su prikupljeni između 2018. i 2019. godine te se smatra da je samo 20% kartica validno. Nacionalni CERT je filtriranjem došao do 191 hrvatske kartice. Poslane su obavijesti nadležnim bankama, kako bi blokirali validne kartice. Osim toga, obaviještena je i Služba kibernetičke sigurnosti pri MUP-u te im je dostavljena kolekcija na analizu. Kroz kolovoz prijavljeno je nekoliko računalno sigurnosnih incidenata u akademskoj zajednici. Većina prijava odnosi se na *UDP flood DDoS* napade. Poslane su prijave izvorima incidenata. CARNET ustanovama člancima poslane su upute kako rekonfigurirati poslužitelj da se više ne koristi za *CLDAP reflection* napade.

U **rujnu** Nacionalni CERT je zaprimio prijavu o phishing kampanji namijenjenoj hrvatskim korisnicima jednog osiguravajućeg društva, s ciljem krađe korisničkih podataka i zaporki. Nacionalni CERT je poslao prijave izvorima incidenta.

4. KVARTAL

#308 incidenata #ucjenjivačke poruke #BEC prijevare #lažne web trgovine #log4j

U četvrtom kvartalu obrađeno je ukupno **308** incidenata. Zabilježen je veći broj BEC prijevara (eng. *business e-mail compromise*). Radi se o vrsti prijevare kod koje se napadač predstavlja kao osoba na rukovodećoj poziciji u nekoj tvrtci te traži hitno plaćanje računa. Prema našim saznanjima napadači su uspješno izvršili BEC prijevare u kojima su hrvatski poslovni korisnici izgubili različite iznose od kojih su neki bili viši od 200.000 kuna. Nacionalni CERT je poslao prijave izvorima te izdao upozorenje.

U **studenom** su aktualne teme bile Crni petak i lažne nagradne igre. Povodom Crnog petka i povećane kupovine putem interneta Nacionalni CERT prikupio je preko 60 lažnih internetskih trgovina koje su se predstavljale kao trgovine poznatih robnih marki. Svoja saznanja i popis trgovina podijelili smo s MUP-om, a na svojim stranicama izdali upozorenje i upute kako prepoznati lažne internetske trgovine i zaštititi se od ovakve vrste prijevare.

Početkom **prosinca** u zajednici je otkrivena 0-day ranjivost Java Apache biblioteke log4j. Iskorištavanje ranjivosti (*Log4Shell exploit*) omogućava potencijalnom udaljenom napadaču izvršavanje proizvoljnog programskog koda ili krađu osjetljivih informacija. Nacionalni CERT je redovito obavještavao korisnike o novostima vezanim uz navedene ranjivosti te radio na masovnom skeniranju IP adresnog prostora u nadležnosti CARNET-a kako bi otkrili ranjivosti i spriječili iskorištavanje istih. Osim toga, objavljene su upute za otkrivanje ranjivih servisa.

4. USLUGE CARNET-OVOG NACIONALNOG CERT-A

4.1. CERT ETA

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu Nacionalni CERT je razvio uslugu CERT ETA 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 ETA usluge je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvatske i regije (tzv. *spameri*), a koji često nisu obuhvaćeni poznatim globalnim listama.

CERT ETA nije zamjena za poznate liste kao što su Spamhaus, SpamCop, Sorbs i sl. Upute za korištenje usluge dostupne su na poveznici https://www.cert.hr/cert_eta/

Praćenjem pokazatelja korištenja usluge vidljivo je da dodatak postavljen na poslužiteljima e-pošte mjesečno stavlja na crnu listu u prosjeku 202 jedinstvene IP adrese i 8 jedinstvenih domena, a broj korisničkih upita za pristigle poruke elektroničke pošte u mjesečnom prosjeku iznosi 692.074.

cert eta

4.2. CERT EPSILON

CERT Epsilon 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 oznaka te ID oznaka. Ova usluga je početkom 2021. zamijenila uslugu "Sigurnosne preporuke" kojom se korisnicima distribuiralo informacije putem mailing lista i stranice cert.hr.

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. Usluga je dostupna na poveznici https://epsilon.cert.hr/

Prema pokazateljima korištenja usluge u protekloj godini ukupan broj korisnika usluge je 133, a ukupan broj posjeta stranici je 1621.

cert epsilon

4.3. PIXI – PLATFORMA ZA PRIKUPLJANJE, ANALIZU I RAZMJENU PODATAKA O RAČUNALNO-SIGURNOSNIM PRIJETNJAMA I INCIDENTIMA

Kako bi se spriječio incident i ubrzao proces njegova zaustavljanja i rješavanja, Nacionalni CERT je u 2021. godini nastavio s razvojem i pokrenuo platformu PiXi za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima. Platforma PiXi služi za prijave značajnih incidenata prema Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga te će, nakon obuhvata korisnika iz svih sektora, zamijeniti dosadašnju proceduru prijave značajnih incidenata koristeći Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga. Tijekom godine Nacionalni CERT je održao edukativne radionice za korisnike iz operatora ključnih usluga, davatelja digitalnih usluga i telekoma.

PiXi

4.4. SIGURNOST CARNET USLUGA

Tijekom 2021. 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, komponenata i usluga CARNET-a;

— usluga izdavanja elektroničkih certifikata (TCS-om);

— provođenje odredaba Programa sigurnosti;

— uvođenje novih tehnologija sa sigurnosnog apekta u informacijski sustav CARNET-a;

— redovita provjera ranjivosti (eng. *Vulnerability Scanning*) ustanova članica CARNET mreže

Tijekom 2021. godine Nacionalni CERT je u sklopu tih aktivnosti:

—provodio penetracijska testiranja važnih CARNET-ovih usluga u sklopu implementacije Programa sigurnosti u CARNET-ove poslovne procese;

— provodio provjeru ranjivosti i provjeru usklađenosti sa standardima (*policy compliance*) CORE mrežnih uređaja CARNET-a

— provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET;

— certificirao aplikacije koje pristupaju sustavu “e-Matica”;

— radio na potpori sigurnosnih aspekata projekta“e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće”.

— radio na projektu izrade CARNET Oblak platforme

4.4.1. 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 57 ustanova iz sustava prosvjete, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže. U 2021. godini provedeno je ukupno 214 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.

4.4.2. TRUSTED CERTIFICATE SERVICE - TCS

CARNET-ov Nacionalni CERT nudi uslugu izdavanja elektroničkih certifikata *(Trusted Certificate Service – TCS)*. Od travnja 2020. godine u suradnji s organizacijom **GÉANT** (prije DANTE i TERENA), CARNET nudi novu uslugu izdavanja elektroničkih certifikata. Izdavatelj certifikata je tvrtka **Sectigo Limited** (umjesto dosadašnje tvrtke **DigiCert**) s kojom je GÉANT zajednica sklopila ugovor.

Vrste certifikata koje CARNET nudi su poslužiteljski certifikati, klijentski S/MIME certifikati, Code Signing certifikati, Document Signing certifikati, Grid certifikati za eScience projekte te Extended Validation (EV) certifikati. U 2021. godini izdano je ukupno 1634 certifikata, što je porast od 5%.

Što se tiče poslužiteljskih certifikata, njih je izdano ukupno 1419 u 2021. godini što je porast u odnosu na 2020. godinu (izdano je 220 poslužiteljskih certifikata više, odnosno 18%, nego prošle godine). U 2021. godini izdano je i 214 klijentskih certifikata, što je pad u odnosu na prošlu godinu u iznosu od 104 certifikata, odnosno 33%.

5. SURADNJA I DJELOVANJE NACIONALNOG CERT-A NA MEĐUNARODNOJ RAZINI

Pored institucija **EU-a** i **NATO-a**, Nacionalni CERT surađuje s i članom je 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 računalno-sigurnosne 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 2021

Hrvatska akademska i istraživačka mreža – CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u četrnaestoj po redu NATO vježbi zaštite NATO i nacionalnih računalnih sustava pod nazivom „**Cyber Coalition 2021**". U petodnevnoj vježbi koja je trajala od 29. studenog do 3. prosinca 2021. godine sudjelovalo je preko 1000 stručnjaka iz područja kibernetičke sigurnosti. Saveznici i partneri su zajedno vježbali kako bi održali visoku razinu kibernetičke sigurnosti zemalja članica NATO-a. Vježba, između ostalog, obuhvaća obranu od zlonamjernog sadržaja (eng. *malware*) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske, a čiji je koordinator bio CARNET. Akademsku zajednicu u vježbi su predstavljali Fakultet elektrotehnike i računarstva Zagreb, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Visoko učilište Algebra, Fakultet prometnih znanosti Zagreb i Pravni fakultet u Osijeku. Sudjelovala su i 4 subjekta iz privatnog sektora (Microsoft Hrvatska, INsig2 d.o.o., INFIGO IS d.o.o., Eduron IS). Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

"Cyber Coalition 2021"

5.2. CSIRT MREŽA

Mreža CSIRT-ova (eng. ***CSIRTs Network***) nastala je temeljem Direktive o mrežnoj i informacijskoj sigurnosti (**NIS direktiva**) 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 te Europske Komisije. Hrvatsku na sastancima zastupa delegacija koju čine stručnjaci iz Nacionalnog CERT-a i Zavoda za sigurnost informacijskih sustava (ZSIS). Na sastancima su predstavljeni rezultati radnih grupa koje su oformljene unutar CSIRT mreže, a koje za cilj imaju unaprjeđenje 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, Europske Komisije, napretku razvoja Europske platforme za razmjenu informacija o računalno-sigurnosnim incidentima – MeliCERTes te o detaljima kibernetičkih vježbi koje se održavaju na EU razini ili ciljano za članove CSIRT mreže. Održana je vježba CyberSOPEx kojom se uvježbavaju standardne operativne procedure CSIRT mreže, suradnja između različitih CSIRT timova te razmjena informacija.

5.3. DSI GOVERNANCE BOARD

Nacionalni CERT od 2018. godine aktivno sudjeluje u radu odbora *CEF Cyber DSI Governance Board* koji je uspostavljen unutar europskog CEF (eng. *Connecting Europe Facility*) programa sufinanciranja za projekte koji se provode u okviru implementacije Europske strategije kibernetičke sigurnosti. Nastavkom aktivnosti projekta Grow2CERT, Nacionalni CERT podržava i implementira usluge i servise nadogradnje i poboljšanja razmjene informacija o kibernetičkim prijetnjama i incidentima na europskoj razini te se pridružuje ostalim europskim projektima na zajedničkoj platformi MeliCERTes koja je ušla u drugu fazu razvoja s projektom SMART 2018/1024. Odbor ima upravljačku ulogu za sve projekte financirane iz CEF programa za kibernetičku sigurnost, usmjerava i vodi voditelje projekata, predstavlja i služi interesima EU kroz praćenje i usmjeravanje suradnje na zajedničkoj platformi, sudjeluje u procesima donošenja odluka po pitanju strategija, politika i aktivnosti unutar CEF programa te izvještava o projektima. Predstavnici Nacionalnog CERT-a sudjelovali su na dva radna sastanka odbora. Na sastancima su predstavljeni rezultati provedenih aktivnosti u sklopu projekta Grow2CERT.

6. SURADNJA I DJELOVANJE NACIONALNOG CERT-A NA NACIONALNOJ RAZINI

6.1. SPORAZUM O POSLOVNOJ SURADNJI S MUP-OM

U 2021. godini nastavlja se suradnja na prevenciji i rješavanju računalnih 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 međusobnu suradnju kako bi uvijek bili spremni na računalno-sigurnosne izazove kojih je svakim danom sve više.

6.2. SPORAZUM O POSLOVNOJ SURADNJI S FER-OM

CARNET nastavlja poslovnu 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 2021. godine kao rezultat suradnje objavljene su recenzije s uputama za ukupno 2 alata te je napisano 3 dokumenta na teme iz područja kibernetičke sigurnosti. Recenzija alata **Ghidra** namijenjena je onima koji se bave reverznim inženjeringom programa. Recenzija alata **Splunk free** namijenjena je administratorima te opisuje kako instalirati i koristiti navedeni alat za centralno prikupljanje, pretragu, analizu i vizualizaciju dnevničkih zapisa (eng. *logs*). Dokumenti **"Sigurnosni rizici Wordpress CMS-a"**, **"Transport Layer Security (TLS) verzija 1.3"** i **"Osnovno sigurnosno ojačavanje Linux poslužitelja"** teme su namijenjene svima koji žele znati više o kibernetičkoj sigurnosti. Posebno valja izdvojiti organizaciju i provedbu drugog CTF natjecanja za srednjoškolce pod nazivom **"Hacknite"** tijekom listopada u sklopu aktivnosti vezanih uz obilježavanje Europskog mjeseca kibernetičke sigurnosti. Za potrebe natjecanja razvijeni su vrlo zanimljivi i izazovni sadržaji koji su izazvali snažnu potporu svih sudionika, a pogotovo učenika srednjih škola. Organiziranjem natjecanja svim zainteresiranim učenicima dana je prilika za učenje o kibernetičkoj sigurnosti. Natjecanje je bilo vrlo uspješno te će se sigurno organizirati i narednih godina. Više o samom natjecanju u poglavlju **6.7**.

6.3. SUDJELOVANJE U RADU TIJELA IZ NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

Tijekom 2021. godine Nacionalni CERT nastavio je aktivno sudjelovati u radu nacionalnih relevantnih tijela proizašlih iz **Nacionalne strategije kibernetičke sigurnosti**: **Nacionalnog vijeća za kibernetičku sigurnost** i **Operativno-tehničke koordinacije za kibernetičku sigurnost**. Uz praćenje provedbe Strategije i Akcijskog plana ovim međuresornim tijelima povjeravaju se i određene zadaće vezane uz upravljanje u kibernetičkim krizama. Sjednice navedenih tijela održavaju se jednom mjesečno (osim u iznimnim situacijama kada je moguće sazvati izvanrednu sjednicu).

6.4. ZAKON I UREDBA O KIBERNETIČKOJ SIGURNOSTI OPERATORA KLJUČNIH USLUGA I DAVATELJA DIGITALNIH USLUGA

U 2021. izmijenjena je i dopunjena **"Nacionalna taksonomija računalno-sigurnosnih incidenata" nastalog temeljem Mjere G.1.1 Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti"**. Nova inačica je u primjeni od početka 2022. i prema njoj se klasificiraju računalno-sigurnosni incidenti na nacionalnoj razini u svojim informacijskim sustavima i računalnim mrežama.

Tijekom 2021. 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.

6.5. SURADNJA S HRVATSKOM UDRUGOM BANAKA

Nacionalni CERT je i u 2021. godini 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. Suradnja s Hrvatskom udrugom banaka započela je i ranije kroz zajedničke mjere iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, radnu skupinu iz projekta GrowCERT i Grow2CERT, no pojavila se i dodatna potreba za jačanjem suradnje zbog Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. 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

6.6. OBILJEŽAVANJE EUROPSKOG MJESECA KIBERNETIČKE SIGURNOSTI

CARNET-ov Nacionalni CERT aktivno je obilježio Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2021. godine proveden je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti, s naglaskom na mrežnu i informacijsku sigurnost te promociju sigurnijeg korištenja interneta za sve korisnike.

Nacionalni CERT je ponovno imao ulogu nacionalnog koordinatora za provedbu Europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti tijekom listopada te je ažurirao sadržaj na stranici https://cybersecuritymonth.eu/countries/croatia

EUROPEAN CYBER SECURITY MONTH

Pod sloganom "Razmisli prije nego klikneš!" teme na kojima je 2021. godine bio naglasak su digitalni trag, kibernetička higijena, internet bonton, prva pomoć za žrtve računalno-sigurnosnih incidenata, siguran rad od kuće i nastava na daljinu. Sukladno navedenim temama pripremljeno je pet najavnih spotova za infografike i infografike na hrvatskom jeziku koji su prezentirani široj javnosti, šest spotova žrtava kibernetičkih napada iz pravog života i četiri video priče o potencijalnom kibernetičkom napadu i obrani od napada.

Najveća aktivnost u Europskom mjesecu kibernetičke sigurnosti bila je kampanja Veliki hrvatski naivci, koja je nakon dvije godine ponovno bila vidljiva korisnicima putem različitih kanala: osim reklamnih sadržaja na mrežnim stranicama, Nacionalni CERT je objavio dva video spota koje su korisnici gledali tijekom listopada na programu HRT-a. Lik Ivane u potrazi za brzom zaradom preuzima zlonamjerni softver, a lik Daniela izgubi novčana sredstva zbog djevojke koju je upoznao na internetu. Osim toga, Nacionalni CERT je izradio deset aktivnosti u obliku interaktivnih sadržaja i igrifikacije za opću javnost.

Teme sadržaja uključuju zanimljive činjenice o kibernetičkoj sigurnosti, igre memorije s ključnim pojmovima u kibernetičkoj sigurnosti i kibernetičkim prijetnjama te kvizovi koji obuhvaćaju phishing prijevare i kibernetičku higijenu.

U studenom je održana panel rasprava „Koliko smo podložni manipulaciji?", na kojoj su sudjelovali predstavnici javnih institucija, privatnog i bankarskog sektora te akademske zajednice, raspravilo se o temama socijalnog inženjeringa, kibernetičkoj higijeni, otkrivanju osobnih i bankovnih podataka, podizanju svijesti o kibernetičkoj sigurnosti te lakovjernosti korisnika interneta u Hrvatskoj. Sudionici rasprave su naglasili važnost brige o kibernetičkoj higijeni svakog korisnika interneta – od vrtića do starije životne dobi.

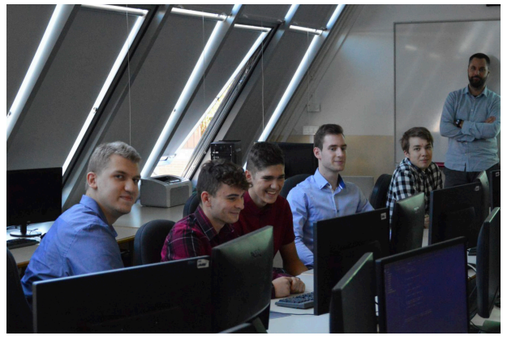
6.7. HACKNITE 2.0 – DRUGO IZDANJE CTF NATJECANJA ZA SREDNJOŠKOLCE

U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je drugo izdanje hrvatskog CTF natjecanja za srednjoškolce, provedeno od 15. do 17. listopada 2021. 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 je bio proširiti svijest o važnosti primjene sigurnosnih mjera te izbjegavanju i ispravljanju mogućih sigurnosnih propusta u programskom kôdu, postavkama ili nekoj drugoj komponenti računalnog sustava.

U natjecanju je sudjelovao 51 srednjoškolski tim iz 18 gradova i 32 srednje škole. Pobjednički tim bio je **tim gospoda** iz Tehničke škole Čakovec.

Učenici su imali prilike puno naučiti, a čime su se iskazali je odlična suradnja između timova i međusobno pomaganje, iako su se nalazili na "suparničkim" stranama. Reakcije na natjecanje su bile vrlo pozitivne te se nadamo da će se i narednih godina natjecanje ovakvog tipa uspješno organizirati i da će učenici koji nisu uspjeli igrati ove godine priliku dobiti u idućem mjesecu kibernetičke sigurnosti. Osim toga, prvih pet timova je imalo priliku sudjelovati na europskom CTF natjecanju **Cybershare Academy for Schools** gdje su postigli izvrsne rezultate i zauzeli prvo i treće mjesto.



Pobjednici Hacknite.hr 2.0: tim gospoda

6.8. DJELOVANJE PUTEM JAVNIH MEDIJA I OBRAĆANJA JAVNOSTI

02/2021 – gostovanje na HRT-u u emisiji Dobro jutro Hrvatska povodom Dana sigurnijeg interneta

02/2021 – sudjelovanje na videokonferenciji "Potraga za boljim internetom" namijenjenoj učenicima i nastavnicima povodom obilježavanja Dana sigurnijeg interneta

09/2021 – gostovanje u regionalnim vijestima HRT-a na temu sigurnosti kupovine na internetu

10/2021 – gostovanje na HRT-u u emisiji Dobro jutro Hrvatska povodom Europskog mjeseca kibernetičke sigurnosti

10/2021 – sudjelovanje na konferenciji CSC21 (*Cyber Security Conference*) u Osijeku s temom na poslovnom dijelu "PiXi – platforma za razmjenu informacija o incidentima i prijetnjama" i temom na tehničkom dijelu konferencije "Predstavljanje platforme PiXi za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim incidentima"

10/2021 – gostovanje na okruglom stolu u sklopu CSC21 konferencije na temu "Kibernetička sigurnost javne infrastrukture"

11/2021 – dva interaktivna izlaganja na konferenciji CUC2021 na teme "Igrifikacija i računalna sigurnost u nastavi" i "Servisi i usluge Nacionalnog CERT-a " te radionica na temu "Pobijedi svoju naivnost i #SurfajSigurnije"

11/2021 – dva webinara za obrazovatelje na teme „Alisa u zemlji TikToka – Sigurnost na društvenim mrežama" i „Zaštita virtualnog identiteta"

11/2021 – sudjelovanje u panel raspravi „Koliko smo podložni manipulaciji?" na temu socijalnog inženjeringa

11/2021 – gostovanje u panel raspravi u sklopu KOM21 konferencije na temu "Kibernetička sigurnost u ključnim uslugama"

12/2021 – gostovanje na dnevniku Nove TV na temu iskorištavanja ranjivosti

— Informiranje javnosti putem web sjedišta Nacionalnog CERT-a (**www.cert.hr**) – 43 309 posjetitelja u 2021. godini. Ove godine posebno valja izdvojiti situacije kada su objavljivana upozorenja prilikom čega je promet značajno premašivao prošlogodišnje brojke

— Informiranje javnosti putem društvenih mreža Facebook (@CERT.hr - 1873 pratitelja) i Twitter (@HRCERT – 1314 pratitelja)

— Dano je više od 8 intervjua i izjava za časopise te tiskane i digitalne medije, npr. Lider, Global novine, Faktograf

7. PROJEKTI

7.1. E-ŠKOLE

U 2021. godini CARNET-ov odjel za Nacionalni CERT provodio je aktivnosti projekta **"e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće"**. Projektni elementi "Sigurnosti" s ciljem postizanja adekvatne razine sigurnosti CARNET mrežne infrastrukture, infrastrukture podatkovnih centara, sigurnost ustanova i javno dostupnih usluga i aplikacija. Provodi se sveobuhvatna procjena usluga i aplikacija razvijenih unutar projekta kako bi se ostvarila njihova spremnost za postavljanje u produkcijsku okolinu. S projektnim partnerom **ICENT** (Inovacijski centar Nikola Tesla) provode se istraživačke aktivnosti s ciljem poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola.

e-Škole

7.2. GROW2CERT

Nacionalni CERT je u 2021. godini nastavio s provedbom projekta sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe (eng. CEF – *Connecting Europe Facility*) pod nazivom **Grow2CERT** – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti (eng. *Increasing maturity of National CERT for stronger cooperation in cybersecurity community*).

Cilj projekta je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Platforma PiXi za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima nadograđena je novim komponentama i puštena u produkciju 3. svibnja 2021. Korisnici usluge su operatori ključnih usluga i davatelji digitalnih usluga sukladno **ZKS-u**, te pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga sukladno **Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga**. Do kraja projekta nacionalna platforma će omogućiti interakciju s MeliCERTes-om koji predstavlja zajednički mehanizam suradnje i razmjene informacija o računalno-sigurnosnim prijetnjama i incidentima na europskoj razini. PiXi platforma služi kao nacionalno mjesto za prikupljanje podataka, razmjenu informacija i brzo djelovanje korisnika računalno-informacijskih sustava u Hrvatskoj kako bi se osiguralo njihovo neometano poslovanje, a time sigurnost usluga koje su od posebne važnosti za odvijanje ključnih društvenih i gospodarskih aktivnosti u Hrvatskoj poput bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture i poslovnih usluga za državna tijela. Usluga je predstavljena na prošlogodišnjim nacionalnim konferencijama posvećenim temama iz kibernetičke sigurnosti (**KOM 21**, **CSC 21**) te na radnim sastancima CSIRT mreže i DSI Governance Boarda za CEF projekte. Razvoj i uspjeh usluge prepoznat je na europskoj razini kao primjer dobre prakse međusektorske suradnje i razvoja povjerenja među dionicima unutar nacionalne zajednice kibernetičke sigurnosti. Za korištenje usluge osposobljeno je ukupno 95 korisnika iz 37 različitih pravnih subjekata, a do kraja godine aktivirano je 112 korisničkih računa.

Nacionalni CERT je proveo niz aktivnosti s ciljem podizanja svijesti opće javnosti o kibernetičkoj sigurnosti putem digitalne kampanje, objava na društvenim mrežama, izradom **digitalnih interaktivnih sadržaja**, organizacijom okruglog stola **„Koliko smo podložni manipulaciji?"** i drugih događanja posvećenih temama kibernetičke sigurnosti tijekom **Europskog mjeseca kibernetičke sigurnosti.**

Poseban naglasak stavljen je na **„kibernetičku higijenu"**, odnosno održavanje visoke razine sigurnosti korisnika interneta uz odgovorno korištenje suvremenih informacijsko-komunikacijskih tehnologija. Opseg projekta čini osam različitih aktivnosti. Uz upravljanje projektom i komunikaciju i vidljivost, ostale aktivnosti odnose se na nadogradnju nacionalne platforme i pripremu za nove interakcije / korištenje komponenti MeliCERTes-a, aktivnosti podizanja svijesti, povećanje razine zrelosti Nacionalnog CERT-a na temelju SIM3 kriterija, poboljšanje kapaciteta osoblja CERT-a i drugih nacionalnih tijela koja sudjeluju u provedbi mjera kibernetičke sigurnosti te nabava opreme i licenci za podizanje ukupne razine kibernetičke sigurnosti. Projekt u vrijednosti većoj od milijun eura provodit će se do kraja lipnja 2022. godine.

grow2cert

Sufinancira Europska unija
Instrument za povezivanje Europe

7.3. CEKOM

Nacionalni CERT sudjeluje u EU projektu Centar kompetencija za kibernetičku sigurnost upravljačkih sustava – **CEKOM**. Cilj trogodišnjeg projekta je povećati konkurentnost hrvatskog gospodarstva poticanjem inovativnosti poslovnog sektora i suradnje sa znanstveno-istraživačkim institucijama u području kibernetičke sigurnosti upravljačkih sustava (uključujući i industrijske upravljačke sustave – eng. *Industrial Control System*, ICS).

Nositelj projekta je tvrtka CS Computer Systems d.o.o., a CARNET / Nacionalni CERT uz KONČAR – Inženjering za energetiku i transport d.d., Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva – FER i tvrtku Hrvatski operator prijenosnog sustava d.o.o., sudjeluje kao partner na projektu.

7.4. CYBER EXCHANGE

U studenom 2018. godine započeo je projekt **„CyberExchange"** u okviru Instrumenta za povezivanje Europe – *Connecting Europe Facility* (CEF). Nositelj projekta je udruženje CZ.NIC iz Češke, a u projektu sudjeluje 10 država Europske unije (Austrija, Hrvatska, Češka, Grčka, Latvija, Luksemburg, Malta, Poljska, Rumunjska i Slovačka). Radi se o dvogodišnjem projektu s ciljem jačanja suradnje između nacionalnih i državnih CSIRT-ova/CERT-ova. CyberExchange je pokrenut radi poboljšanja odaziva na sve učestalije prijetnje kibernetičkoj sigurnosti te naglašava važnost prekogranične suradnje u njihovom suzbijanju. Osim toga, važna je i stručnost osoba koje rade u području kibernetičke sigurnosti stoga se provodi razmjena djelatnika CERT-ova/CSIRT-ova tijekom koje individualni članovi pojedinih timova imaju priliku razmijeniti iskustva te unaprijediti svoju stručnost. Projektom se također stavlja fokus na implementaciju softverskih alata koje su razvili timovi uključeni u projekt kako bi se koristili na dobrobit cijele sigurnosne zajednice. U 2021. godini naš stručnjak je u dvotjednoj posjeti **CERT.pl-u** (poljskom nacionalnom CERT-u) učio o analizi zlonamjernog sadržaja i proučavao njihove alate i procese koje koriste u obradi računalno-sigurnosnih incidenata. Cyber Exchange projekt više je puta produljen zbog nemogućnosti alternativne provedbe projektnih aktivnosti (online razmjene) te se planira njegov završetak 30.lipnja 2022. godine.

Cyber Exchange

Sufinancira Europska unija
Instrument za povezivanje Europe

8. ZAKLJUČAK

Tijekom 2021. godine CARNET-ov Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenta i smanjenja štete u slučaju njihovog nastanka.

Prema statistikama može se zaključiti kako je broj prijavljenih incidenata manji čime je obrađeno 29% incidenata manje u odnosu na prošlu godinu. To možemo pripisati većoj vidljivosti Nacionalnog CERT-a u javnosti i stalnim aktivnostima podizanja svijesti javnosti o ugrozama koje dolaze s interneta te širenju suradnje s drugim CERT-ovima, hosting providerima i ISP-evima. Broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu smanjio se za 23%. Što se tiče broja registriranihbotova vidi se blagi pad, no broj botova po danu se najčešće kreće nešto ispod 2000 što ne predstavlja razliku u odnosu na prethodne godine. Velika promjena odnosi se i na porast broja incidenata tipa malware URL koji je u 2021. godini ponovno nakon pet godina došao na 3. mjesto.

U svibnju 2021. godine u produkciju je puštena platforma PiXi za razmjenu informacija o incidentima I prijetnjama. Svrha ove platforme je stvaranje krugova povjerenja te dijeljenje informacija s ciljem prevencije širenja pojedinog incidenta i ublažavanja njegovih posljedica. Korisnici usluge su operatori ključnih usluga i davatelji digitalnih usluga sukladno ZKS-u, te pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga sukladno Pravilniku o načinu i rokovima provedbe mjera zaštite sigurnosti i cjelovitosti mreža i usluga te ostala relevantna tijela u Republici Hrvatskoj iz područja kibernetičke sigurnosti.

CARNET-ov Nacionalni CERT nastavio je razvijati suradnju s institucijama izvan Republike Hrvatske, kao što su drugi CERT timovi, s institucijama EU-a i NATO-a te s ostalim tijelima unutar Republike Hrvatske, a sve u svrhu razvitka zajedničkih interesa u području kibernetičke sigurnosti. Tijekom 2021. godine uspješno je sudjelovao u NATO-ovoj Cyber Coalition vježbi, gdje je Republika Hrvatska sudjelovala u svojstvu igrača. Vježba je, između ostalog, obuhvaćala obranu od zlonamjernog sadržaja (eng. malware) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti. Osim toga Nacionalni CERT sudjelovao je u vježbi CyberSOPEx kojom se uvježbavaju standardne operativne procedure CSIRT mreže, suradnja između različitih CSIRT timova te razmjena informacija.

CARNET je ponovno aktivno obilježavao Europski mjesec kibernetičke sigurnosti. Tijekom listopada 2021. godine Nacionalni CERT proveo je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti, s naglaskom na mrežnu i informacijsku sigurnost te promociju sigurnijeg korištenja interneta za sve korisnike. Nacionalni CERT ove je godine imao ulogu nacionalnog koordinatora za provedbu Europske kampanje za podizanje svijesti o kibernetičkoj sigurnosti tijekom listopada. U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je drugo izdanje hrvatskog CTF natjecanja za srednjoškolce koje se provodilo od 15. do 17. listopada 2021. godine. U natjecanju je sudjelovao 51 srednjoškolski tim iz 18 gradova i 32 srednje škole.

Javnost je o aktivnostima informirana putem web sjedišta Nacionalnog CERT-a (**www.cert.hr**) – 43 309 posjetitelja u 2021. godini, a posebno valja izdvojiti situacije kada su objavljivana upozorenja prilikom čega je promet značajno premašivao prošlogodišnje brojke. Informirana je javnost putem društvenih mreža Facebook (**@CERT.hr** - 1873 pratitelja) i Twitter (**@HRCERT** – 1314 pratitelja). Odrađeno je više od 8 intervjua i izjava za časopise te tiskane i digitalne medije, npr. Poslovni lider, 24 sata, Indeks, Večernji list, Jutarnji list, T-portal te je snimljeno nekoliko reportaža za HRT i Novu TV.

CARNET-ov odjel za Nacionalni CERT nastavio je s provedbom aktivnosti u projektu "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće". U projektnim elementima „Sigurnost" s ciljem postizanja primjerene razine sigurnosti CARNET mrežne infrastrukture, infrastrukture podatkovnih centara, sigurnosti ustanova i javno dostupnih usluga i aplikacija. Provodi se sveobuhvatna procjena usluga i aplikacija razvijenih unutar projekta kako bi se ostvarila njihova spremnost za postavljanje u produkcijsku okolinu. S projektnim partnerom ICENT (Inovacijski centar Nikola Tesla) provode se istraživačke aktivnosti s ciljem poboljšanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola.

Nacionalni CERT je u 2021. godini nastavio s provedbom projekta Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti sufinanciranog sredstvima Europske unije putem Instrumenta za povezivanje Europe. Cilj projekta je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Između ostalog, projektom se nastavlja razvoj platforme PiXi za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima na nacionalnoj razini. Uz aktivni doprinos članova radne skupine i institucija, dionika Nacionalne strategije za kibernetičku sigurnost, u prosincu je izmijenjena i dopunjena Nacionalna taksonomija računalno-sigurnosnih incidenata koja je u primjeni od 1. siječnja 2022. godine.

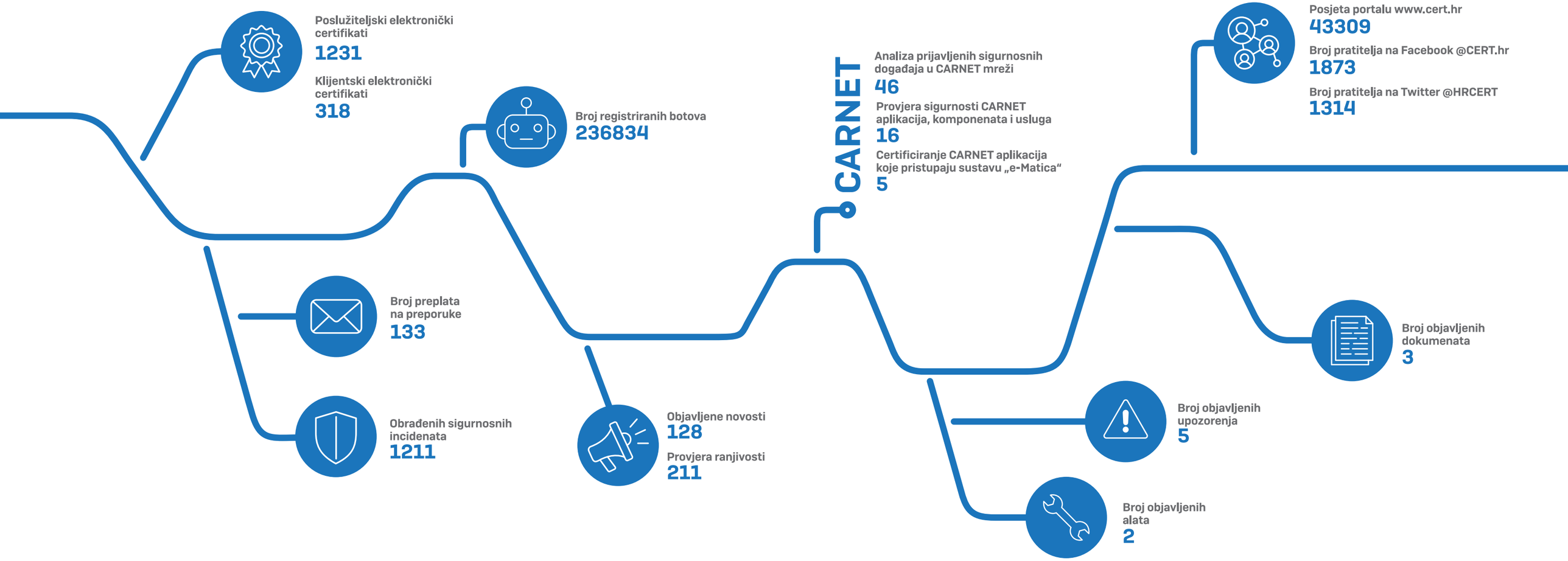
Zaključno, Nacionalni CERT je u 2021. godini ostvario značajne pomake na području nacionalne i međunarodne suradnje, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

9. MALI POJMOVNIK RAČUNALNO-SIGURNOSNIH 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 incidenata koji se spominju u ovom izvještaju.

POJAM	KRATKI OPIS
Bot/Botnet	Zaraženo računalo/mreža zaraženih računala
C&C	Komandni i kontrolni poslužitelj koji upravlja mrežom zaraženih računala
Phishing	Masivno zasipanje velikog broja osoba porukama u kojima se na prijevaru traži odavanje tajnih podataka
Spam	Neželjena elektronička poruka poslana zbog namjere oglašavanja raznog propagandnog sadržaja, ili u svrhu phishing napada, ili kao sredstvo distribucije poveznica do zlonamjernog softvera
Malware	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika
Web Defacement	Izmjena izgleda stranica web sjedišta
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.
Phishing URL	Poveznica do lažne *web* stranice koja oponaša legitimnu stranicu na kompromitiranom *web* sjedištu s ciljem krađe povjerljivih korisničkih podataka
Malware URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu
Spam URL	*Spam* sadržaj na kompromitiranom web sjedištu koji se distribuira kroz *spam* poruke
DoS	Napad uskraćivanja usluge
Spyware	Vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole
Backdoor alati	Alati koji omogućuju drugom korisniku da se služi žrtvinim računalom dok je žrtva spojena na internet, bez znanja žrtve
SQL injection napadi	Napad umetanjem SQL koda koji iskorištava ranjivosti na sloju baze podataka
Brute force napadi	Testiranje svih kombinacija slova, brojeva i posebnih znakova s ciljem otkrivanja zaporki

NACIONALNI CERT U BROJKAMA



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**, računalno-sigurnosne incidente prijavite na **incident@cert.hr**,a za upite medija kontaktirajte nas na **press@carnet.hr**.

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

Ovaj dokument pripremljen je uz financijsku podršku Europske unije. Sadržaj rada izražava mišljenje autora te ni na koji način ne izražava mišljenje i stavove Europske unije.

Hrvatska akademska
i istraživačka mreža – CARNET
Josipa Marohnića 5, 10000 Zagreb, Hrvatska
tel: +385 1 6661 616, mail: ured@carnet.hr

Podrška:
tel: +385 1 6661 555
mail: helpdesk@carnet.hr