2022.

CERT.hr

GODIŠNJI IZVJEŠTAJ

CARNET

SADRŽAJ

SADRŽAJ

15 GODINA U ZAŠTITI KIBERNETIČKOG PROSTORA RH

NACIONALNI CERT (CERT.HR) JE ODJEL HRVATSKE AKADEMSKE I ISTRAŽIVAČKE MREŽE – CARNET KOJI SE BAVI OBRADOM RAČUNALNO-SIGURNOSNIH INCIDENATA, PODIZANJEM SVIJESTI I EDUKACIJOM O KIBERNETIČKOJ SIGURNOSTI GRAĐANA REPUBLIKE HRVATSKE.

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 30.07.2007. 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. 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.

Nacionalni CERT je obilježio 15 godina svoga djelovanja u kojem su poduzete brojne radnje kako bi hrvatski kibernetički prostor bio sigurniji:

- obrađeno više od 71.000 računalno-sigurnosnih incidenata,
- obrađeno više od 42.000 abuse incidenata,
- provedeno više od 3.000 provjera ranjivosti,
- izdano više od 82.000 sigurnosnih upozorenja,
- izdano oko 9.000 elektroničkih certifikata,
- objavljeno više od 3.000 novosti,
- objavljeno 900 recenzija alata,
- objavljeno više od 200 stručnih dokumenata.

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 sukladno Zakonu o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (ZKS) za sektore bankarstva, infrastrukture financijskog tržišta, digitalne infrastrukture, dio poslovnih usluga za državna tijela i davatelje digitalnih usluga.

1. MJERE NACIONALNOG CERT-A

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

Tijekom 2022. godine Nacionalni CERT provodio je 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 CARNET-ov 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 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 (poslužiteljskih i klijentskih);
- 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 o kibernetičkoj sigurnosti;
- 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.

BROJ IZVRŠENIH PROAKTIVNIH MJERA U 2022. GODINI

Dokumenti	3
Novosti	161
Broj pretplata na CERT Epsilonu	162
Broj provjera ranjivosti	210
Broj izdanih elektroničkih certifikata	2.322

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 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

Tijekom 2022. godine obrađeno je ukupno 1.296 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tip incidenata su **phishing, scam i phishing URL.**

Promjena u odnosu na prošlu godinu je povećanje broja korisničkih prijava računalno-sigurnosnih incidenata od ukupno 7% u usporedbi s 2021. godinom. Pretpostavka je da je do povećanja došlo uslijed rezultata kampanji, edukacija i ostalih aktivnosti podizanja svijesti građana, veće medijske i javne zauzetosti za teme iz područja kibernetičke sigurnosti i posebno sigurnosti i zaštite krajnjih korisnika. Također, stalni trend porasta broja prijava i obrađenih incidenata rezultat je veće javne vidljivosti Nacionalnog CERT-a, ali i neprestanog usavršavanja alata za detekciju kompromitacija i dodavanje novih izvora informacija o prijetnjama i incidentima. Zbog velike ovisnosti o tehnologijama i sve sofisticiranijih metoda napadača i u narednim godinama očekujemo trend laganog povećanja ukupnog broja obrađenih incidenata.

Velika promjena odnosi se na porast broja incidenata koji su klasificirani kao scam koji je u 2022. godini došao na drugo mjesto tipova prijavljenih incidenata. Razlog tome je povećan broj prijava takvih incidenata od strane građana za koji pretpostavljamo da se dogodio uslijed objavljivanja upozorenja o scam i phishing kampanjama na mrežnim i društvenim stranicama Nacionalnog CERT-a

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 38,7% u odnosu na prethodnu godinu.

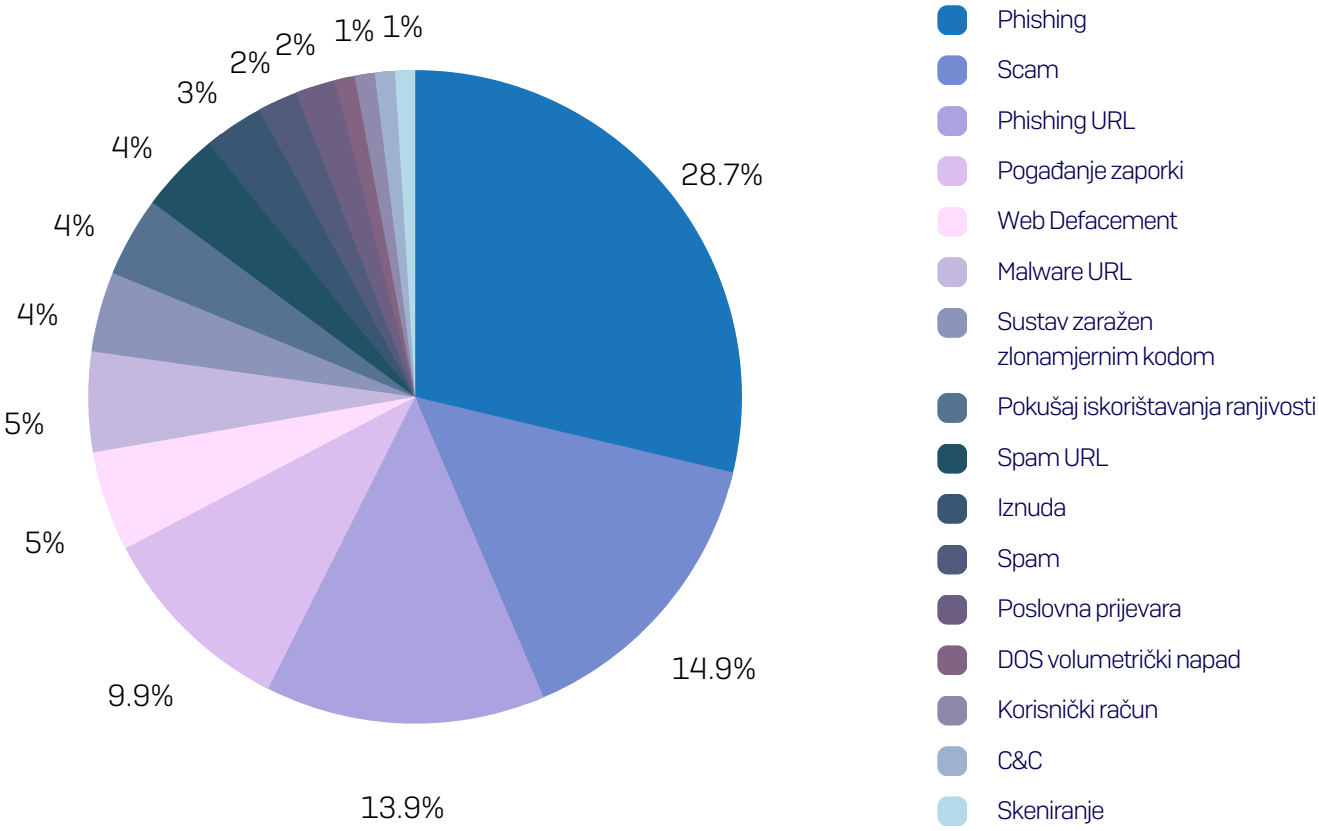
PRIKAZ INCIDENATA PO TIPU U 2022. GODINI

Phishing	371	▲
Scam	191	▲
Phishing URL	186	▼
Pogađanje zaporki	130	▲
Web Defacement	71	▼
Malware URL	67	▼
Sustav zaražen zlonamjernim kodom	54	▼
Pokušaj iskorištavanja ranjivosti	48	▼
Spam URL	48	▲
Iznuda	34	—
Spam	27	▲
Poslovna prijevara	19	—
DoS - Volumetrički napad	17	▼
Korisnički račun	11	▼
C&C	7	▲
Skeniranje	5	▲
Ispad usluge (eng. Outage)	4	▼
DoS - napad na aplikacijskom sloju	2	▲
Zlonamjerno web sjedište	2	—
Ostalo	2	▼
Zlonamjerno rudarenje kriptovalute	1	▲
Hoax	1	▼
UKUPNO	**1.296**	▲

Prema trendu kretanja tipova incidenata vidljivo je da je veći dio kategorija u padu, no sveukupni broj incidenata je u porastu. Razlog tome je veći porast broja određenih tipova incidenata.

2.2 RASPODJELA INCIDENATA PO TIPU

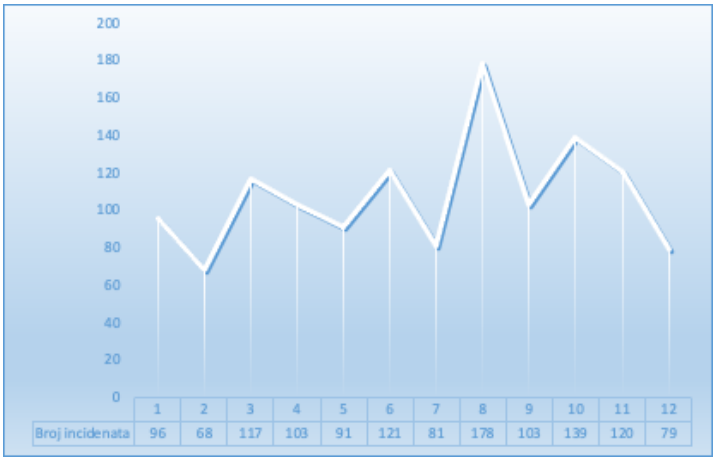
Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2022. godini, koji su zabilježeni u sustavu za obradu incidenata.



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

2.3 TRENDOVI POJAVA INCIDENATA NA POSLUŽITELJIMA U 2022. GODINI

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



MJESEČNI PRIKAZ BROJA INCIDENATA NA POSLUŽITELJIMA U 2022. GODINI

Na grafičkom prikazu vidljiv je skok broja incidenata u kolovozu. Razlog povećanja broja incidenata u kolovozu je povećan broj phishing kampanja koje su ciljale korisnike mobilnih bankarstava hrvatskih banaka. U napadima se koristila tematika uvođenja eura kao službene valute u Hrvatskoj gdje se korisnika putem poveznice navodilo na preuzimanje nove inačice aplikacije, ali se radilo o tome da napadač želi preuzeti pristup mobilnom bankarstvu korisnika.

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). U odnosu na 2021. godinu, u 2022. godini značajno se smanjio broj registriranih zaraženih računala u Hrvatskoj. 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.

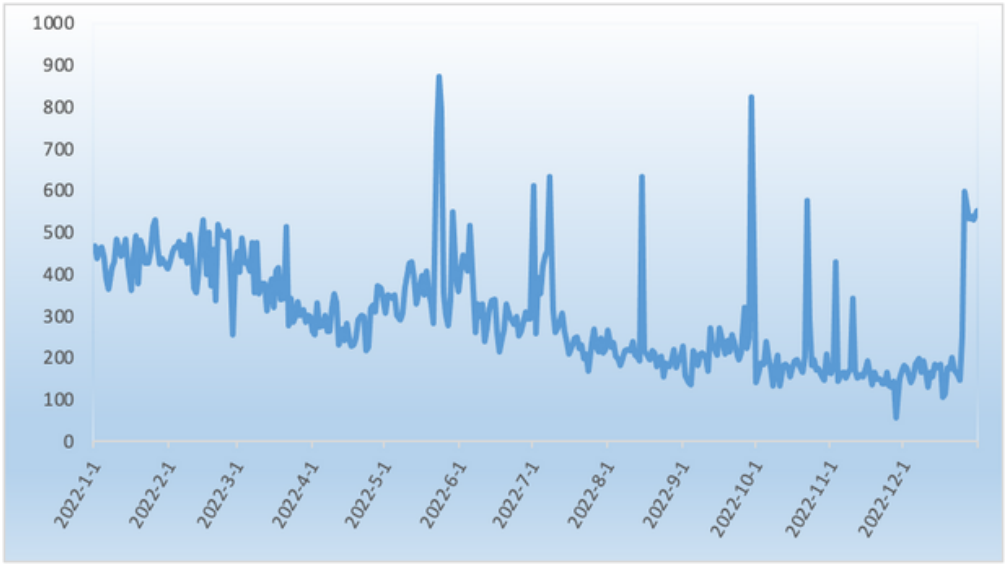
U tablici u nastavku prikazano je deset najčešće prijavljivanih botova prema tipu (vrsti zlonamjernog sadržaja) u 2022. godini, koji su bili proslijeđeni davateljima internetskih usluga.

DESET NAJČEŠĆE PRIJAVLJIVANIH BOTOVA U RH

gamut	**18.263**
flubot	**12.165**
mirai	**11.192**
necurs	**6.542**
andromeda	**4.367**
malware-generic	**3.089**
unknown	**2.748**
qsnatch	**2.467**
sality	**1.326**
likely-rat-adwind	**1.267**

Zbroj zabilježenih botova prema tipu (vrsti zlonamjernog sadržaja) tijekom 2022. godine iznosi 68.879, što je smanjenje od 70,9 % u odnosu na 2021. godinu.

BROJ ZABILJEŽENIH BOTOVA PO DANIMA U 2022. GODINI



Prema trendu kretanja poznatih botova u Hrvatskoj može se zaključiti da se uglavnom kreću oko 300 botova dnevno, što je manje od prošle godine. Srednja vrijednost broja botova po danu za 2022. godinu iznosila je 301,5 što je smanjenje za više od 1.090 botova prosječno po danu u odnosu na 2021. 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 2022. godine, služba CARNET Abuse obradila je ukupno 5.411 incidenata. 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 savjetuje da skeniraju računalo i očiste ga od zlonamjernog sadržaja.

3. ZNAČAJNIJI INCIDENTI, OTKRIVENE RANJIVOSTI I DOGAĐAJI

KVARTAL 1

#281 incident #Emotet #sextortion #Ukrajina

U prvom kvartalu 2022. godine obrađen je 281 računalno-sigurnosni incident. U siječnju je detektiran povećan broj phishing poruka sa zlonamjernim privitcima. Napadači su lažirali polja pošiljatelja tako da izgledaju kao legitimne privatne i poslovne adrese elektroničke pošte. Privitci su sadržavali zapakirane i nezapakirane Microsoft Excel i Word datoteke, koje pri otvaranju pokreću makro naredbe, preuzimaju i instaliraju zlonamjerni softver Emotet. Nacionalni CERT je izdao upozorenje za javnost uz analizu privatne tvrtke te poslao prijavu pružateljima usluga na kojima se nalazi payload zlonamjernog softvera.

Također je zaprimljen povećan broj prijava lažnih ucjenjivačkih "sextortion" poruka kojima napadač pokušava iznuditi novčanu korist od žrtve. Nacionalni CERT je poslao prijave davatelju usluga s čijeg su se poslužitelja distribuirale poruke. Dodatno, objavljeno je upozorenje na mrežnim stranicama i društvenim mrežama. Kampanja ucjenjivačkih poruka se nastavila te je Nacionalni CERT objavio novo upozorenje s informacijama o incidentu.

U prvom kvartalu 2022. godine, Nacionalni CERT, kao član CSIRT Network zajednice, povećava međunarodnu suradnju i komunikaciju zbog povećanog broja kibernetičkih napada usmjerenih prema Ukrajini. Za vrijeme povećane suradnje, u Hrvatskoj nema primijećenih računalno-sigurnosnih incidenata koji se mogu povezati s napadima na Ukrajinu. Osim toga, izdani su savjeti za podizanje svijesti o kibernetičkoj sigurnosti i priopćenje za javnost o stanju kibernetičke sigurnosti za vrijeme hibridnog ratovanja u Ukrajini.

KVARTAL 2

#315 incidenata #smishing #BEC prijevare #apartmani

U drugom kvartalu 2022. godine obrađeno je 315 računalno-sigurnosnih incidenta.

Detektirana je smishing kampanja u kojoj se napadač predstavlja kao tvrtka koja pruža poštanske usluge, pritom koristeći URL (eng. Uniform Resource Locator) identičan službenom, ali na .com vršnoj domeni. Nakon što je Nacionalni CERT prijavio incident izvoru, napadač je promijenio pružatelja usluga udomljavanja (eng. Hosting Provider) te ponovno aktivirao domenu. Brzom reakcijom CERT-a i pružatelja usluga, smishing kampanja je uspješno zaustavljena.

Osim što su napadači koristili smishing tehniku kod lažnih poštanskih usluga, Nacionalni CERT je zaprimio prijavu računalno-sigurnosnog incidenta gdje se putem SMS-a distribuira phishing poveznica na kojoj se od potencijalne žrtve traži da aktivira korisnički račun za korištenje usluga jedne hrvatske banke.

Nacionalni CERT je zaprimio prijavu poslovne prijevare tipa BEC (eng. Business Email Compromise). Napadač je kompromitirao poslovni račun zaposlenika tvrtke te kroz prethodnu, stvarnu komunikaciju s poslovnim partnerom i distributerom, pokušao izmijeniti podatke za uplatu. Napad je pravovremeno zaustavljen, a Nacionalni CERT je proslijedio prijavu i policiji.

U drugom kvartalu, Nacionalni CERT je zaprimio prijavu pokušaja phishing prijevare, gdje se napadač predstavlja kao iznajmljivač apartmana putem platforme za rezervaciju smještaja. Napadač se neposredno nakon rezervacije javlja gostu putem mobilne aplikacije za razmjenu poruka te šalje phishing poveznicu za plaćanje smještaja. Poslana je prijava za deaktivaciju phishing stranice te oglasa na platformi.

Krajem drugog kvartala, zbog smanjenog obujma kibernetičkih napada prema EU članicama, CSIRT Network zajednica vraća suradnju na standardnu razinu, ali naglašava važnost dijeljenja informacija o računalno-sigurnosnim incidentima i prijetnjama povezanih s Ukrajinom.

KVARTAL 3

#362 incidenta #AgentTesla #Nagradne igre #AveMaria #Euro

U trećem kvartalu 2022. godine obrađeno je 362 računalno-sigurnosna incidenta. Nacionalni CERT i dalje prati sve kanale komunikacije s CSIRT Network zajednicom te se po potrebi obavještava korisnike putem mrežne stranice i društvenih mreža o mogućim kibernetičkim napadima povezanim sa situacijom u Ukrajini. Važniji pokazatelji kompromitacije koji su zabilježeni kod napada na Ukrajinu redovito se dijele putem PiXi platforme.

Zaprimljene su bile prijave o phishing kampanjama koje ciljaju korisnike hrvatskog digitalnog oglasnika i poštanskih usluga. Radi se o phishing stranicama na kojima se nalazi obrazac za krađu bankovnih podataka. Zlonamjerne stranice redovito se uklanjaju, međutim napadači mijenjaju domenu i pružatelje usluga i poveznice ponovno postaju aktivne. Osim toga, u trećem su kvartalu bile aktualne phishing kampanje koje također oponašaju poznate međunarodne kurirske službe, a poruke sadrže zlonamjerne privitke. Napadači navode korisnike putem elektroničke pošte na preuzimanje privitka (npr. račun, narudžbenica, dostavnica), a zapravo preuzimaju zlonamjerni softver Agent Tesla koji neovlašteno preuzima osjetljive informacije putem FTP (eng. File Transfer Protocol) poslužitelja.

Nacionalni CERT je zaprimio nekoliko prijava phishing poveznica koje su se distribuirale putem mobilne aplikacija za razmjenu poruka. Phishing poveznice oponašaju lažne nagradne igre poznatih trgovačkih lanaca te prikupljaju osobne i financijske podatke korisnika.

Osim toga, bila je aktualna phishing kampanja gdje se napadač predstavljao kao policijska službenica za odnose s javnošću. Phishing poruka je sadržavala zlonamjerni privitak Ave Maria koji je komunicirao s C&C (eng. Command and Control) poslužiteljem. Zbog brzog širenja phishing kampanje, izdano je upozorenje na mrežnoj stranici i društvenim mrežama.

U trećem kvartalu 2022. godine zabilježen je i povećan broj phishing kampanja koje ciljaju korisnike aplikacija za mobilno, digitalno, odnosno internet bankarstvo.

Napadači su krenuli iskorištavati tematiku dvojnog iskazivanja cijena zbog uvođenja eura kao službene valute u Hrvatskoj. Napadač se predstavljao kao banka, a potencijalnu žrtvu putem elektroničke pošte obavještava o novoj inačici aplikacije zbog uvođenja eura. Napadač navodi žrtvu na otvaranje poveznice na kojoj "potvrđuje" točnost telefonskog broja kako bi preuzeo novu inačicu aplikacije. Nakon unosa telefonskog broja, otvara se novi obrazac za unos aktivacijskog kôda. Žrtva unosi aktivacijski kôd koji dobiva putem aplikacije nakon promjene uređaja. Podaci u obrascu se šalju napadaču, koji tako dobiva pristup aplikaciji mobilnog bankarstva žrtve, kao i svim funkcionalnostima same aplikacije. Na posljednjem koraku, korisnika se obavještava da zbog ažuriranja sustava mobilna aplikacija neće biti u funkciji naredna 24 sata te da će novi aktivacijski kôd za prijavu biti poslan na adresu elektroničke pošte. Zbog velikog broja prijava, izdano je upozorenje na mrežnoj stranici i društvenim mrežama Nacionalnog CERT-a.

KVARTAL 4

#338 incidenata #scam #sextortion #BidenCash #Malware #WalletConnect

U četvrtom kvartalu 2022. godine obrađeno je 338 računalno-sigurnosnih incidenata. Bile su aktivne scam kampanje u kojima se napadač predstavlja kao načelnik policije te pokušava zastrašiti potencijalnu žrtvu navodeći je da odgovori na priloženi "sudski poziv" upućen zbog djela kibernetičkog kriminala, nakon čega slijedi iznuda. Nacionalni CERT izdao je upozorenje na mrežnoj stranici te društvenim mrežama zbog povećanog broja prijava.

Osim toga, ponovno je bilo aktivno nekoliko ucjenjivačkih "sextortion" kampanja usmjerenih prema hrvatskim korisnicima. Nacionalni CERT je u četvrtom kvartalu izdao dva upozorenja, u listopadu i studenom, uz primjere takvih poruka. Poruke su bile strojno prevedene te sadržavale gramatičke i pravopisne pogreške.

Polje pošiljatelja bilo je lažirano tako da izgleda kao da je poruka poslana sa žrtvinog računa, a u nekim slučajevima se radilo i o stranim adresama elektroničke pošte. Sadržaj i naslovi poruka mijenjaju se iz kampanje u kampanju, kao i iznosi uplate koje napadač traži. U većini slučajeva radi se o jednom kripto novčaniku, ali ponekad napadači koriste više kripto novčanika u istoj kampanji kako bi bilo teže ući im u trag.
U četvrtom kvartalu, zaprimljene su prijave korisnika za phishing poruke koje sadrže zlonamjerne privitke - LokiBot, Remcos, FormBook, Artemis, Nanocore i Warzone. Nacionalni CERT redovito radi na analizi zlonamjernih privitaka, kao i na otkrivanju i prijavi C2 poslužitelja koji upravljaju zlonamjernim kôdom.

Nacionalni CERT je temeljem članka u medijima o curenju podataka bankovnih kartica pronašao i analizirao bazu podataka „Biden Cash" te obavijestio sve nadležne hrvatske bankarske i financijske institucije čiji su korisnici pronađeni u bazi. Osim toga, baza je podijeljena svim zainteresiranim članovima CSIRT Network zajednice.

Zaprimljena je prijava phishing poruke s phishing URL-om koji imitira uslugu za kripto novčanike „Wallet Connect". U poruci napadač od potencijalne žrtve traži verifikaciju korisničkog računa zbog problema s kripto novčanikom. Cilj phishing napada je krađa privatnog ključa kripto novčanika koji se sastoji od 12 ili 24 riječi.

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

CERT ETA nije zamjena za poznate liste kao što su Spamhaus, SpamCop, Sorbs i sl.

Praćenjem pokazatelja korištenja usluge vidljivo je da dodatak postavljen na poslužiteljima e-pošte mjesečno stavlja na crnu listu u prosjeku 23 jedinstvene IP adrese i 6 jedinstvenih domena, a broj korisničkih upita za pristigle poruke elektroničke pošte u mjesečnom prosjeku iznosi 975.446.

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.

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 162, a ukupan broj posjeta stranici je 3241.

cert epsilon

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

PiXi

Kako bi se spriječio incident i ubrzao proces njegova zaustavljanja i rješavanja, Nacionalni CERT je 2021. godine pokrenuo Nacionalnu 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 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 2022. godine održane su četiri edukativne radionice za korisnike iz operatora ključnih usluga iz sektora poslovnih usluga za državna tijela, zdravstva te prometa.

Održana je prezentacija o PiXi usluzi SI-CERT-u (slovenskom nacionalnom CERT-u) i drugim institucijama u Sloveniji koje se bave kibernetičkom sigurnosti u svrhu širenja informacija o samoj platformi, prikazu njenih funkcionalnosti te razmjene dobrih praksi.
Početkom lipnja, platforma PiXi je spojena na MeliCERTes2 platformu u svrhu razmjene informacija o računalno-sigurnosnim incidentima u zajednici CERT-ova Europske unije i CSIRT Networka.
Krajem lipnja održana je završna konferencija Grow2CERT projekta na kojoj su predstavljeni cjelokupni rezultati uz prikaz funkcionalnosti same PiXi platforme.

U listopadu su korisnici PiXi platforme informirani o nadogradnji i novoj funkcionalnosti za primanje IntelMQ izvješća u kojima se prikupljaju i obrađuju sigurnosni podaci o prijetnjama. Glavni cilj je pružiti osobama koje reagiraju na incidente jednostavan način prikupljanja i obrade obavještajnih podataka o prijetnjama.

4.4 SIGURNOST CARNET USLUGA

Tijekom 2022. 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);
- 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-a kao ustanove radi unaprjeđenja sigurnosti.

Tijekom 2022. godine Nacionalni CERT je u sklopu tih aktivnosti:

- provodio penetracijska testiranja (18) važnih CARNET-ovih usluga u sklopu implementacije Programa sigurnosti u CARNET-ove poslovne procese;
- 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;
- radio na razradi sigurnosnih aspekata projekta e-Sveučilišta;
- radio na projektu BrAIn;
- radio na projektu uspostave eksperimentalne kvantne komunikacijske infrastrukture.

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 62 ustanove iz sustava prosvjete, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže. U 2022. godini provedeno je ukupno 210 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

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 2022. godini izdano je ukupno 2322 certifikata, što je porast od 42% u odnosu na broj izdanih certifikata u 2021. godini.

Što se tiče poslužiteljskih certifikata, njih je u 2022. godini izdano ukupno 2171, što je 752 izdana certifikata više nego 2021. godine, odnosno porast od 53%. U 2022. godini izdan je i 151 klijentski certifikat, što je 45 certifikata manje nego 2021. godine, odnosno 29% manje.

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 EUROPE 2022

U organizacije Agencije Europske unije za kibernetičku sigurnost (ENISA), 8. i 9. lipnja 2022. godine održana je vježba Cyber Europe. Paneuropska vježba obuhvatila je stručnjake iz 29 zemalja Europske unije i Europskog udruženja slobodne trgovine (EFTA) te agencije i institucije EU, ENISA-u, CERT institucija, tijela i agencija Europske unije (CERT-EU), Europol i Europsku agenciju za lijekove (EMA).

Vježbe Cyber Europe omogućavaju analizu naprednih incidenata u području kibernetičke sigurnosti te rješavanje složenih situacija u pogledu kontinuiteta poslovanja i upravljanja krizom. Ove godine, fiktivni scenarij obuhvatio je napad na infrastrukturu i usluge zdravstvenog sustava uz prijetnju objave osobnih medicinskih podataka u više zemalja Europske unije te kampanju dezinformiranja i diskreditiranja. Koordinatori vježbe na nacionalnoj razinu su predstavnici Nacionalnog CERT-a te CERT-a Zavoda za sigurnost informacijskih sustava. U vježbu su bili uključeni predstavnici Ministarstva zdravstva, Agencije za lijekove i medicinskih proizvoda (HALMED) te malih i velikih bolnica.

5.2 VJEŽBA CYBER COALITION 2022

Hrvatska akademska i istraživačka mreža - CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u petnaestoj po redu NATO vježbi zaštite NATO-a i nacionalnih računalnih sustava pod nazivom „Cyber Coalition 2022".

U petodnevnoj vježbi koja je trajala od 28. studenog do 2. prosinca 2022. 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. Scenariji na vježbi simulirali su ugroze iz stvarnog života kao što su napadi na električne mreže, programe i sredstva NATO-a i Saveznika tijekom vojnih operacija. 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, pravna je skupina osiguravala donošenje odluka u skladu s međunarodnim pravom i praksom te poduzimanje pravnih mjera protiv počinitelja. CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u pravnom scenariju te su koordinirali sudjelovanje igrača i igračica iz privatnog sektora i akademske zajednice.

S više od 60 sudionika postignut je rekord sudjelovanja predstavnika ovih sektora u obrani kibernetičkog prostora. Iz privatnog sektora u vježbi su sudjelovale tvrtke: SPAN d.d., Microsoft Hrvatska d.o.o., Insig2 d.o.o., Infigo IS d.o.o., Infobip d.o.o., EDURON IS d.o.o. Iz akademske zajednice sudjelovali su: Fakultet elektrotehnike i računarstva Zagreb, Fakultet elektrotehnike, računarstva i informacijskih tehnologija Osijek, Fakultet prometnih znanosti Zagreb, Pravni fakultet Osijek, Zavod za informatiku Osijek 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 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 CARNET-ovog odjela za Nacionalni CERT i CERT-a 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.

5.4 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 European 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 2022. 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-ov Nacionalni CERT 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 2022. godine kao rezultat suradnje objavljena su ukupno 3 dokumenta na teme iz područja kibernetičke sigurnosti. Dokumenti "Pregled protokola za privatnost DNS prometa", "Pegasus" i "Zaštita od DDoS napada" "namijenjeni su svima koji žele znati više o kibernetičkoj sigurnosti.

Posebno valja izdvojiti organizaciju i provedbu trećeg CTF natjecanja za srednjoškolce pod nazivom "Hacknit3" 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. Nakon završetka natjecanja je podignuta CTF platforma na kojoj zainteresirani učenici mogu vježbati. Natjecanje je bilo vrlo uspješno te će se sigurno organizirati i narednih godina. Više o samom natjecanju i platformi u poglavlju 6.7.

6.3 SUDJELOVANJE U RADU TIJELA IZ NACIONALNE STRATEGIJE KIBERNETIČKE SIGURNOSTI

Tijekom 2022. godine Nacionalni CERT nastavio je aktivno sudjelovati 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). Započeo je proces izrade nove nacionalne strategije za područje kibernetičke sigurnosti u kojem je Nacionalni CERT preuzeo ulogu vođenja procesa za područje podizanja svijesti i edukacije o kibernetičkoj sigurnosti.

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

Tijekom 2022. 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 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.

HRVATSKA UDRUGA BANAKA
CROATIAN BANKING ASSOCIATION

Međusektorska suradnja vrlo je važna u borbi protiv kibernetičkih incidenata. Suradnja s Hrvatskom udrugom banaka započela je kroz provedbu mjera iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, radnu skupinu iz projekta GrowCERT i Grow2CERT, te je ojačana 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.

6.6 OBILJEŽAVANJE EUROPSKOG MJESECA KIBERNETIČKE SIGURNOSTI (ECSM)

CARNET-ov Nacionalni CERT aktivno je obilježio jubilarni deseti Europski mjesec kibernetičke sigurnosti. Za tu prigodu objavljena je video kompilacija s postignućima i dojmovima zemalja članica. Tijekom listopada 2022. godine proveden je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti.

Nacionalni CERT je 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
Pod sloganom "Razmisli prije nego klikneš!" 10. ECSM se bavio temama phishing i ransomware napada. Iako je kampanja namijenjena svim uzrastima, naglasak je stavljen na osobe starije od 40 godina, a koje se nalaze u radnom odnosu.

10th anniversary EUROPEAN CYBER SECURITY MONTH

Kampanja je najavljena već krajem rujna, a u prvoj polovici listopada objavljivani su sadržaji o phishingu te u drugoj polovici sadržaji o ransomware napadima. U svrhu podizanja svijesti i upoznavanja građana s ovim prijetnjama kreirani su video spotovi, infografike i drugi edukativni materijali sa savjetima za prepoznavanje i zaštitu od ovih prijetnji.

Za vrijeme ECSM-a djelatnici Nacionalnog CERT održali su webinar za učitelje o zaštiti pojedinca i podataka u digitalnom okruženju, predavanje za djelatnike Hrvatske narodne banke, predavanje učenicima OŠ Bogumila Tonija iz Samobora te govorili o kibernetičkoj sigurnosti na CARNET-ovoj konferenciji za korisnike u Šibeniku. Prigodno je kreirana i "Sigurna knjižica" Nacionalnog CERT-a u kojoj se nalaze osnovne informacije o temama iz područja kibernetičke sigurnosti poput najčešći tipova incidenata, kibernetičkoj higijeni, kriptografiji, steganografiji, igrifikaciji u području obrazovanja te digitalnoj forenzici.

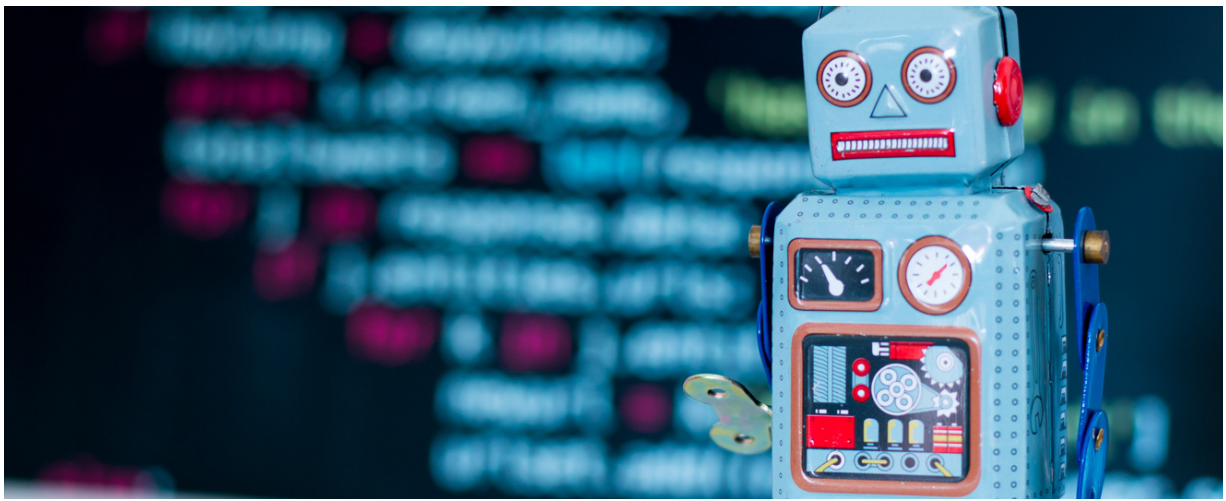
6.7 HACKNIT3 – TREĆE IZDANJE CTF NATJECANJA ZA SREDNJOŠKOLCE

U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je treće izdanje hrvatskog CTF natjecanja za srednjoškolce, provedeno od 14. do 16. listopada 2022. 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.
U natjecanju je sudjelovalo 270 učenika u 54 srednjoškolska tima iz 33 srednje škole. Pobjednički tim bio je tim null iz Gimnazije Andrije Mohorovičića Rijeka s osvojenim maksimalnim brojem bodova i prije isteka vremena. Višak vremena iskoristili su za pisanje uputa za rješavanje zadataka samog natjecanja koje su naknadno javno objavili na svom blogu.

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.
Ove godine pokrenuta je i Hacknite CTF platforma na kojoj se učenici, nakon registracije svojim @skole.hr računom, mogu pripremati za buduća Hacknite natjecanja. Platforma sadrži zadatke sa svih dosadašnjih natjecanja, a učenici mogu pratiti i svoj rank na tablici rezultata.

Hrvatska je prvi put sudjelovala na European Cyber Security Challenge-u (ECSC) s nacionalnim timom sastavljenim od pet srednjoškolaca i pet studenata Fakulteta elektrotehnike i računarstva. ECSC se 2023. godine održava u Norveškoj, a u budućnosti će HACKNITE služiti i kao selekcijsko natjecanje za formiranje tima koji će predstavljati Hrvatsku na europskoj razini.



6.8 DAN SIGURNIJEG INTERNETA

Dan sigurnijeg interneta 2022. Nacionalni CERT je u suradnji s Udrugom „Suradnici u učenju“ i drugim partnerima obilježio cjelodnevnom videokonferencijom “Potraga za boljim internetom” s ciljem podizanja kompetencija za sigurno korištenje interneta i ostalih digitalnih tehnologija.

Na konferenciji su bile obrađene teme sigurnosti na internetu, zaštite virtualnog identiteta i osobnih podataka, edukacije o kibernetičkoj sigurnosti, programiranju, poteškoćama i izazovima koje donosi udaljeno učenje te druge slične teme. Nacionalni CERT je u svojim prezentacijama upoznao sudionike s virtualnim identitetom, digitalnim tragom, vrijednostima i koristima podataka, koje su vrste prijevara s kojima se susrećemo na internetu, kako ih prepoznati i od njih se zaštititi. Kroz povijesni prikaz porijekla i značenja riječi hakiranje i haker, prikazana je etika hakiranja i pojašnjeno kako hakeri nisu uvijek “zločesti” već da se mogu baviti i preventivnim testiranjem sustava kako bi se onemogućilo njihovo neovlašteno korištenje.

Veliki naglasak konferencije usmjeren je na učenike te njihovo obrazovanje o sigurnosti i ugrozama na internetu. Sukladno tome, Nacionalni CERT pozvao je osnovne škole na sudjelovanje u obilježavanju Dana sigurnijeg interneta izradom stripova na tri teme: 1. Dobri i loši digitalni tragovi, 2. Kako zamišljam hakera i što on radi, 3. Osmisli cyber heroja i moći kojima brani internet. Pozivu se odazvalo više od 700 učenika, koji su u timovima do 5 članova izradili više od 200 stripova.

6.9 DJELOVANJE PUTEM JAVNIH MEDIJA I OBRAĆANJA JAVNOSTI

DJELOVANJE PUTEM JAVNIH MEDIJA

Nacionalni CERT je tijekom godine zaprimio brojne medijske upite za koje su pripremljeni informativni članci o temama poput lažnih web trgovina, internetskih prevara, sextinga, osvetničkoj pornografiji, kibernetičkim incidentima u vrijeme pandemije i zaštiti, hakerskim napadima i hakerima, kibernetičkom ratovanju, Europskom mjesecu kibernetičke sigurnosti, projektima i djelovanju Nacionalnog CERT-a. Uz pisane medije zabilježena su brojna gostovanja u televizijskim i radio emisijama posvećenima temama iz kibernetičke sigurnosti.

SUDJELOVANJE NA KONFERENCIJAMA I PREDAVANJA

Predstavnici Nacionalnog CERT-a sudjelovali su na brojnim događanjima na kojima su predstavljene razne teme iz područja kibernetičke sigurnosti: konferencija u suradnji s MUP-om povodom obilježavanja Europskog mjeseca kibernetičke sigurnosti, predstavljanje Nacionalnog CERT-a na Job Fair-u u organizaciji Fakulteta elektrotehnike i računarstva i Kluba studenata elektrotehnike, konferencija tvrtke Verso Altima. Predstavnici Nacionalnog CERT-a održali su predavanje i sudjelovali u raspravi na okruglom stolu: Izazovi obrazovanja stručnjaka kibernetičke sigurnosti na konferenciji CSC 2022. u Osijeku. Na konferenciji za medije povodom obilježavanja Europskog mjeseca kibernetičke sigurnosti (ECSM), u organizaciji Službe kibernetičke sigurnosti Ravnateljstva policije i Odjela za Nacionalni CERT Hrvatske akademske i istraživačke mreže – CARNET predstavljeni su izazovi za kibernetičku sigurnost građana i tvrtki u Hrvatskoj.

Nacionalni CERT sudjelovao je na panelu u sklopu Regionalne konferencije o kibernetičkom nasilju i kibernetičkoj sigurnosti s posebnim naglaskom na mlade i žene u organizaciji Europske mreže za inicijativu Hrvatske – ENIH i Pravobraniteljice za ravnopravnost spolova u suradnji s NATO-m.
Krajem godine na konferenciji „Jačanje otpornosti i EU perspektiva" u organizaciji Zavoda za sigurnost informacijskih sustava održana je prezentacija „PIXI – platforma za prijavu incidenata sa značajnim učinkom".

EDUKACIJE I MREŽNI SEMINARI

Nacionalni CERT je tijekom godine održavao predavanja za različite ciljne skupine. U suradnji s Agencijom za odgoj i obrazovanje organiziran je mrežni seminar za učitelje informatike na kojem su predstavljene teme: Što znači biti kibernetički siguran? Kako prepoznati kibernetičke prijetnje i zaštititi se? Što je socijalni inženjering? U prosincu je održan mrežni seminar za učitelje informatike i računarstva na kojem je Nacionalni CERT predstavio dvije teme: „Etičko hakiranje" i „CTF natjecanja za srednje škole".

Za učenike OŠ Sveti Petar Orehovec i učenike iz partnerskih zemalja u okviru projekta u okviru projekta KA 229 Erasmus+ projekta Strengthen Online Security for Students na temu mobilnosti Online data privacy risks: the more we know the safer!!! održano je predavanje o malware-u i phishingu.
U rujnu u sklopu programa 11. Znanstvenog piknika održano je predavanje „Hoće li me netko hakirati?". U okviru projekta e-Škole održan je mrežni seminar „Primjena mjera zaštite pojedinca i podataka u digitalnom okruženju za hrabre".

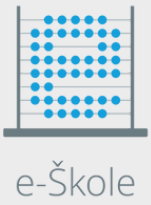
Nacionalni CERT je na CARNET-ovoj konferenciji za korisnike CUC 2022 održao tri predavanja na teme: Sigurnost školskog računala, Zaštita u digitalnom okruženju i Poboljšanje informacijske sigurnosti škola.

Informiranje javnosti provodi se putem:
- web sjedišta Nacionalnog CERT-a kojeg je 2022. godine posjetilo ukupno 177 533 posjetitelja;
- društvenih mreža Facebook (2038 pratitelja) i Twitter (1434 pratitelja).

7. PROJEKTI

Nacionalni CERT je sudjelovao u provedbi četiri projekata sufinancirana sredstvima Europske unije: "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće", "Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti" i kao partner na projektima CEKOM (Centar kompetencija za kibernetičku sigurnost upravljačkih sustava) i CyberExchange.

7.1 E-ŠKOLE



U 2022. godini CARNET-ov 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" provode se s ciljem postizanja adekvatne 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 poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola. Nacionalni CERT je u listopadu tijekom Europskog mjeseca kibernetičke sigurnosti održao edukaciju pod nazivom Primjena mjera zaštite pojedinca i podataka u digitalnom okruženju za hrabre.

7.2 GROW2CERT

Nacionalni CERT je u lipnju 2022. godine završio 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 bio je povećati pripravnost Nacionalnog CERT-a za odgovor na kibernetičke prijetnje i incidente. Nacionalna platforma za razmjenu informacija o računalno-sigurnosnim prijetnjama i incidentima (PiXi) 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.

PiXi je omogućila interakciju s MeliCERTes-om koji predstavlja zajednički mehanizam suradnje i razmjene informacija o računalno-sigurnosnim prijetnjama i incidentima na europskoj razini.

PiXi 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, energetike, prijevoza, zdravstvenog sektora, opskrbe vodom za piće i njezina distribucija, infrastrukture financijskog tržišta, digitalne infrastrukture i poslovnih usluga za državna tijela te davatelja digitalnih usluga. Usluga je predstavljena na brojnim europskim i nacionalnim konferencijama posvećenim temama iz kibernetičke sigurnosti 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 PiXi platforme osposobljeno je više od 200 pojedinaca kroz ciklus od deset radionica i aktivirano je 229 korisničkih računa iz 89 različitih institucija i organizacija.

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, nacionalnom koordinacijom aktivnosti povodom 10. godišnjice obilježavanja Europskog mjeseca kibernetičke sigurnosti.

Rezultat projekta su i ojačani kapaciteti Nacionalnog CERT-a, povećane kompetencije zaposlenika i postignuta viša razina zrelosti temeljem SIM3 kriterija. Na završnom događanju projekta okupila se zainteresirana publika kojoj su predstavljeni rezultati projekta.

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).

7.4 CYBER EXCHANGE

U lipnju 2022. godine završio je projekt „CyberExchange" sufinanciran sredstvima Instrumenta za povezivanje Europe – Connecting Europe Facility (CEF). Nositelj projekta bilo je udruženje CZ.NIC iz Češke, a u projektu je sudjelovalo 10 država Europske unije (Austrija, Hrvatska, Češka, Grčka, Latvija, Luksemburg, Malta, Poljska, Rumunjska i Slovačka). Cilj projekta bio je jačanje suradnje između nacionalnih i državnih CSIRT-ova/CERT-ova kako bi se poboljšao odaziv na sve učestalije prijetnje kibernetičkoj sigurnosti te naglasila važnost prekogranične suradnje u njihovom suzbijanju.

Cyber Exchange

U projektu su bile realizirane brojne razmjene osoblja između CERT-ova kako bi se ulagalo u stručnost osoba koje rade u području kibernetičke sigurnosti. Razmjenama su individualni članovi pojedinih timova imali priliku razmijeniti iskustva te unaprijediti svoju stručnost. Timovi uključeni u projekt podijelili su iskustva i znanja o softverskim alatima koje su razvili i koje koriste. U lipnju je provedena dvodnevna table-top kibernetička vježba u organizaciji Nacionalnog CERT-a u kojoj su sudjelovali projektni partneri iz devet zemalja EU. Osim što su prošetali splitskom rivom razgovarali su o izazovima kibernetičke sigurnosti te razmijenili iskustva i najbolje prakse iz svojih zemalja.

8. ZAKLJUČAK

Tijekom 2022. godine CARNET-ov Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere, obilježeno je 15 godina od osnutka NCERT-a i 10. godišnjica Europskog mjeseca kibernetičke sigurnosti, provođeni su brojni projekti, održane edukacije i medijska pojavljivanja, provjeravani sustavi te izdavanja upozorenja, a sve u svrhu očuvanja sigurnosti kibernetičkog prostora RH i zaštite građana.

Prema statistikama može se zaključiti kako je razina prijavljenih incidenata u laganom porastu te je obrađeno 7% više incidenata nego 2021. godine. To možemo pripisati većoj vidljivosti Nacionalnog CERT-a u javnosti, stalnim aktivnostima podizanja svijesti javnosti i pisanju upozorenja o aktualnim ugrozama koje dolaze s interneta. Broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu smanjio se za 38,7%. Što se tiče broja registriranih botova vidi se značajan pad. Broj botova po danu se kretao oko 300, a uzmemo li u obzir da je 2021. godine prosjek iznosio nešto manje od 2000 botova dnevno, vidimo da je došlo do značajnog pada od čak 70,9%. Velika promjena odnosi se i na rast broja incidenta tipa scam, koji je u 2022. godini skočio na 2. mjesto.

Nastavljena je nadogradnja i razvoj PiXi platforme, njezino spajanje na MeliCERTes2 platformu kako bi se povezala i s ostalim CERT-ovima. Održane su četiri edukacije za nove članove PiXi platforme, a za sve buduće snimljeni su edukativni video materijali.

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 2022. godine uspješno je sudjelovao u NATO-ovoj Cyber Coalition vježbi, gdje je Republika Hrvatska sudjelovala u svojstvu igrača. Vježba je okupila više od 1000 sudionika iz cijelog svijeta, a CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u pravnom scenariju te su koordinirali sudjelovanje igrača i igračica iz privatnog sektora i akademske zajednice.

CARNET-ov Nacionalni CERT aktivno je sudjelovao u obilježavanju 10. po redu Europskog mjeseca kibernetičke sigurnosti. Tijekom listopada 2022. godine Nacionalni CERT proveo je niz aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti, s naglaskom na teme phishinga i ransomwarea. U sklopu obilježavanja Europskog mjeseca kibernetičke sigurnosti organizirano je treće izdanje hrvatskog CTF natjecanja za srednjoškolce. Ovogodišnje natjecanje obilježio je dosad najveći broj prijavljenih natjecatelja. Natjecalo se čak 270 učenika u 54 tima iz 33 škole. Portal Nacionalnog CERT-a www.cert.hr tijekom 2022. godine posjetilo je 53.217 korisnika s ukupno 177.533 pregleda stranica. Objavljena je 161 novost iz područja kibernetičke sigurnosti.

Nacionalni CERT u 2022. godini bilježi daljnji porast pratitelja na društvenim mrežama Facebook @CERT.hr – 2038 pratitelja i Twitter @HRCERT – 1435 pratitelja. Odrađeno je više od 20 intervjua i izjava za časopise te tiskane i digitalne medije, kao što su Nova TV, N1, Jutarnji list, HRT, Faktograf, Lider i dr. Osim medijskih gostovanja, održani su brojni webinari, gostovanja na konferencijama i predavanja s ciljem podizanja svijesti građana o kibernetičkoj sigurnosti.

U 2022. godini CARNET-ov 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". Provodili su se projektni elementi "Sigurnosti", sveobuhvatna procjena usluga i aplikacija razvijenih u sklopu projekta, a s projektnim partnerom ICENT provode se istraživačke aktivnosti s ciljem poboljšavanja i održavanja kibernetičke sigurnosti informacijskih sustava e-Škola. U listopadu, tijekom Europskog mjeseca kibernetičke sigurnosti, je održana edukacija pod nazivom „Primjena mjera zaštite pojedinca i podataka u digitalnom okruženju za hrabre“.
Nacionalni CERT je uspješno završio s provedbom projekta Grow2CERT – Povećanje zrelosti Nacionalnog CERT-a za čvršću suradnju u zajednici kibernetičke sigurnosti. 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.

Zaključno, Nacionalni CERT je u 2022. 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.

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.

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	Upravljački poslužitelj za nadzor i upravljanje računalima koja su dio botneta.
DoS	Napad uskraćivanja usluge.
Malware	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika.
Malware URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu.
Payload	Malware 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 koda koji iskorištava ranjivosti na sloju baze podataka.
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, a računalno-sigurnosne 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	2.171
Klijentski elektronički certifikati	151
Broj preplata na preporuke	162
Broj registriranih botova	68.879
Obrađenih sigurnosnih incidenata	1.296
Analiza prijavljenih sigurnosnih događaja u CARNET mreži	47
Provjera sigurnosti CARNET aplikacija, komponenata i usluga	18
Certificiranje CARNET aplikacija koje pristupaju sustavu „e-Matica“	2
Objavljene novosti	161
Provjera ranjivosti	210
Broj objavljenih upozorenja	11
Broj objavljenih dokumenata	3
Posjeta portalu www.cert.hr	177.533
Broj pratitelja na Facebook @CERT.hr	2.038
Broj pratitelja na Twitter @HRCERT	1.435

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)