2023.

CERT.hr

GODIŠNJI IZVJEŠTAJ

CARNET

SADRŽAJ

Uvod

Tijekom 2023. godine Nacionalni CERT je provodio svoje proaktivne i reaktivne mjere, brojne projekte, održao edukacijske i druge aktivnosti posvećene podizanju svijesti o kibernetičkoj sigurnosti, informirao korisnike o kibernetičkim prijetnjama, ranjivostima i incidentima kroz medijska pojavljivanja i objave upozorenja putem društvenih mreža i web sjedišta te je redovito provjeravao sustave u svojoj nadležnosti te informirao korisnike o pronađenim ranjivostima i mjerama koje je potrebno provesti u svrhu očuvanja sigurnosti kibernetičkog prostora RH i zaštite građana.

Statistički podaci pokazuju blagi pad od 4,63% u broju obrađenih incidenata u 2023. uspoređujući s pokazateljima iz 2022. godine, no zabilježene su nove tehnike napada i sofisticiranije kampanje poput korištenja QR kôda i korištenja relevantnih informacija koje su poslužile za bolje ciljanje i vjerodostojnije iskorištavanje građana poput povrata poreza, subvencija za troškove stanovanja ili prelaska na euro.

Incidenti tipa *phishing* činili su čak 49% svih obrađenih incidenata. Broj otkrivenih kompromitiranih *web* sjedišta je u značajnom porastu u odnosu na prethodnu godinu. Otkrivena su 142 sustava zaražena zlonamjernim kôdom, što je 263% više nego 2022. godine. U broju registriranih botova također je vidljiv značajan rast. Broj botova po danu kretao se oko 800 dok je u 2022. godini taj prosjek bio oko 300 botova.

Nastavljena je nadogradnja i razvoj PiXi platforme koja je postala središnje mjesto za prijavu i izvještavanje o incidentima sa značajnim učinkom za operatore ključnih usluga i davatelje digitalnih usluga u RH.

Neke usluge poput CERT ETA i CERT EPSILON preimenovane su u prepoznatljivije nazive CERT Spamblok i CERT CVE i njihove funkcionalnosti dodatno su nadograđene I bolje prilagođene korisnicima.

Nacionalni CERT surađuje s brojnim institucijama i organizacijama na nacionalnoj, europskoj i međunarodnoj razini kao što su drugi CERT timovi, institucije EU-a i NATO-a u svrhu postizanja zajedničkih ciljeva u području kibernetičke sigurnosti. CARNET i Nacionalni CERT sudjelovali su u NATO-ovoj Cyber Coalition vježbi u dijelu scenarija svojih nadležnosti, u tehničkom dijelu, pravnom scenariju i kriznoj komunikaciji te su koordinirali sudjelovanje igrača i

igračica iz privatnog sektora i akademske zajednice. Vježba je okupila više od 1300 sudionika iz 35 zemalja članica NATO-a i partnerskih zemalja, akademske zajednice i industrije. Sudionici su uključivali najnovijeg saveznika Finsku, zemlje partnere Švedsku, Gruziju, Irsku, Japan, Južnu Koreju, Švicarsku, Ukrajinu, kao i Europsku uniju.

CARNET-ov Nacionalni CERT aktivno sudjeluje u obilježavanju Europskog mjeseca kibernetičke sigurnosti provedbom niza aktivnosti s ciljem podizanja razine svijesti hrvatskih građana o kibernetičkoj sigurnosti. Provedeno je četvrto nacionalno CTF natjecanje za srednjoškolce H4cknite u kojem je sudjelovalo 315 učenika I učenica iz 40 škola.

Prošle godine bilježimo porast posjeta portalu Nacionalnog CERT-a www.cert.hr s 105.169 korisnika s ukupno 185.536 pregleda stranica. Objavljene su 193 novosti iz područja kibernetičke sigurnosti. Povećan je broj posjetitelja I pratitelja na društvenim mrežama Facebook @CERT.hr – 2212 pratitelja i Twitter @HRCERT – 1485 pratitelja.

U porastu je interes medija za djelovanje Nacionalnog CERT-a koji je sudjelovao u 30 intervjua i izjava za časopise te tiskane i digitalne medije, kao što su Nova TV, N1, Jutarnji list, HRT, Faktograf, Lider i dr. Uz medijsku pojavnost djelatnici Nacionalnog CERT-a održali su brojne webinare, gostovanja na konferencijama i predavanja s ciljem podizanja svijesti građana o kibernetičkoj sigurnosti.

U 2023. godini CARNET je završio s provedbom projekta "e-Škole no započeo i s novim projektima: BrAIn, CroQCI i e-Sveučilišta. U listopadu 2023. Godine Odlukom Vlade, Hrvatska akademska i istraživačka mreža – CARNET određena je kao Nacionalno koordinacijsko središte za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti (NKS).

Zaključno, Nacionalni CERT je u 2023. godini ostvario značajne pomake na području nacionalne i međunarodne suradnje, medijske prisutnosti, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

Nataša Glavor
Pomoćnica ravnatelja za Sektor – Nacionalni CERT

1. Mjere Nacionalnog CERT-a

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

Tijekom 2023. 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 putem 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;

Proaktivne mjere u brojkama u 2023. godini

Izdani dokumenti	2
Novosti	193
Broj pretplata na CERT CVE	156
Broj provjera ranjivosti	81
Broj izdanih elektroničkih certifikata	2501

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 2023. godine zaprimljeno je i obrađeno ukupno 1236 prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a. Vodeći tipovi incidenata su ***phishing***, ***phishing URL*** i ***scam.***

Promjena u odnosu na prošlu godinu je smanjenje broja računalno-sigurnosnih incidenata od ukupno 4,63%. Razlog tome je velik broj zabilježenih phishing kampanja u kojima je izvor računalno-sigurnosnih incidenata bio isti, te su

tretirani kao jedan incident. Velika promjena odnosi se na **porast broja incidenata koji su klasificirani kao *Sustav zaražen zlonamjernim kôdom*,** u usporedbi s prošlom godinom ovaj tip incidenta je porastao za 263% odnosno s 54 incidenta na 142. Razlog ovom porastu je povećan broj vanjskih prijava te prijave zaprimljene kroz suradnju s CSIRT zajednicom.

Također je zabilježen i porast broja incidenata tipa *phishing i phishing URL*, u usporedbi s prošlom godinom. Ukupan broj incidenata ove klasifikacije porastao je za 53, što označava uvećanje od 9,52%, čime incidenti tipa phishing čine 49% svih incidenata. Razlog tome je povećan broj prijava takvih incidenata od strane građana za koji pretpostavljamo da se dogodio uslijed objavljivanja upozorenja o *phishing* kampanjama na mrežnim i društvenim stranicama kao i veće javne vidljivosti Nacionalnog CERT-a. Isto tako, zabilježene su phishing kampanje u kojima napadači imitiraju legitimne servise koje koristi velik broj građana.

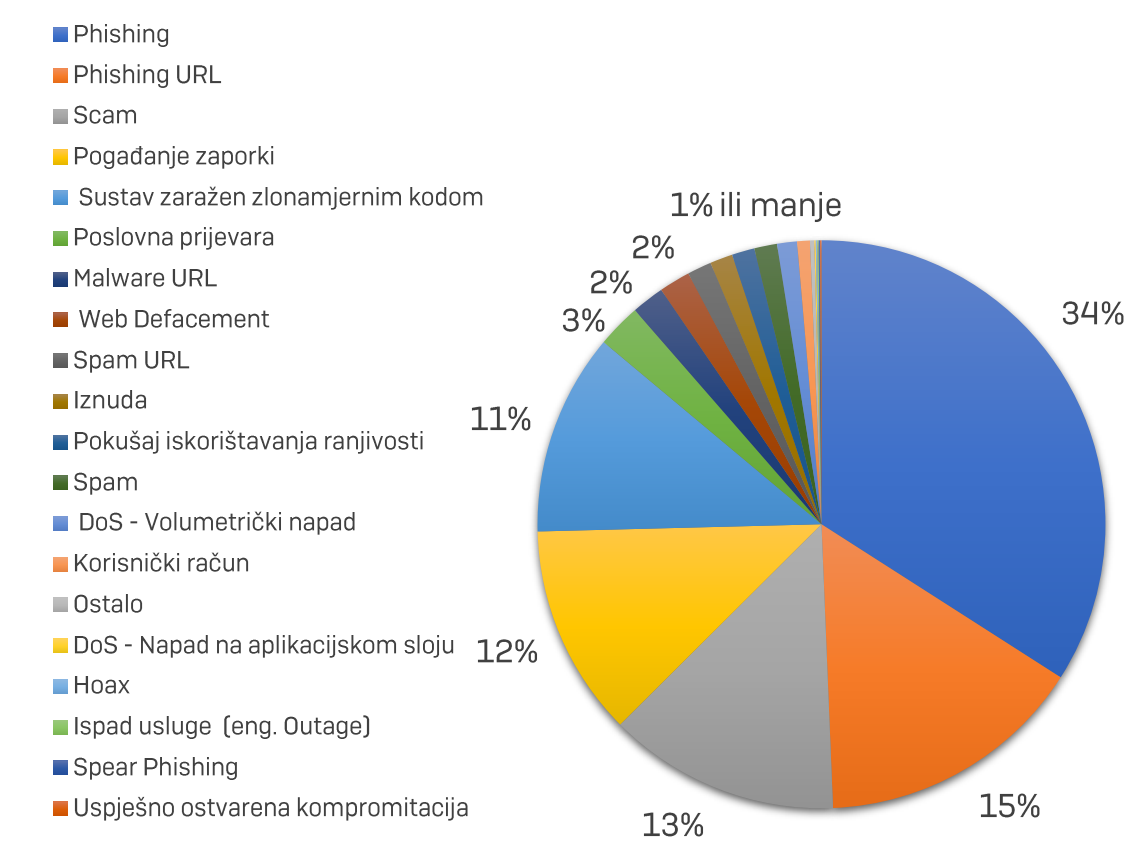
Prikaz incidenata po tipu u 2023. godini

Phishing	421	▲
Phishing URL	189	▲
Scam	163	▼
Pogađanje zaporki	149	▲
Sustav zaražen zlonamjernim kôdom	142	▲
Poslovna prijevara	31	▲
Malware URL	23	▼
Web Defacement	22	▼
Spam URL	17	▼
Iznuda	16	▼
Pokušaj iskorištavanja ranjivosti	16	▼
Spam	16	▼
DoS - Volumetrički napad	14	▼
Korisnički račun	9	▼
Ostalo	3	▲
DoS - Napad na aplikacijskom sloju	1	▼
Hoax	1	–
Ispad usluge (eng. Outage)	1	▼
Uspješno ostvarena kompromitacija	1	–
Spear Phishing	1	▲
UKUPNO	1236	▼

Prema trendu kretanja tipova incidenata vidljivo je da je veći dio kategorija u padu, što nas upućuje na to da se napadači još više no prije okreću prema financijski isplativim vrstama kibernetičkog kriminaliteta.

2.2. Raspodjela incidenata po tipu

Sljedeći grafikon prikazuje udjele incidenata po tipu u 2023. godini, koji su zabilježeni u sustavu za obradu incidenata.

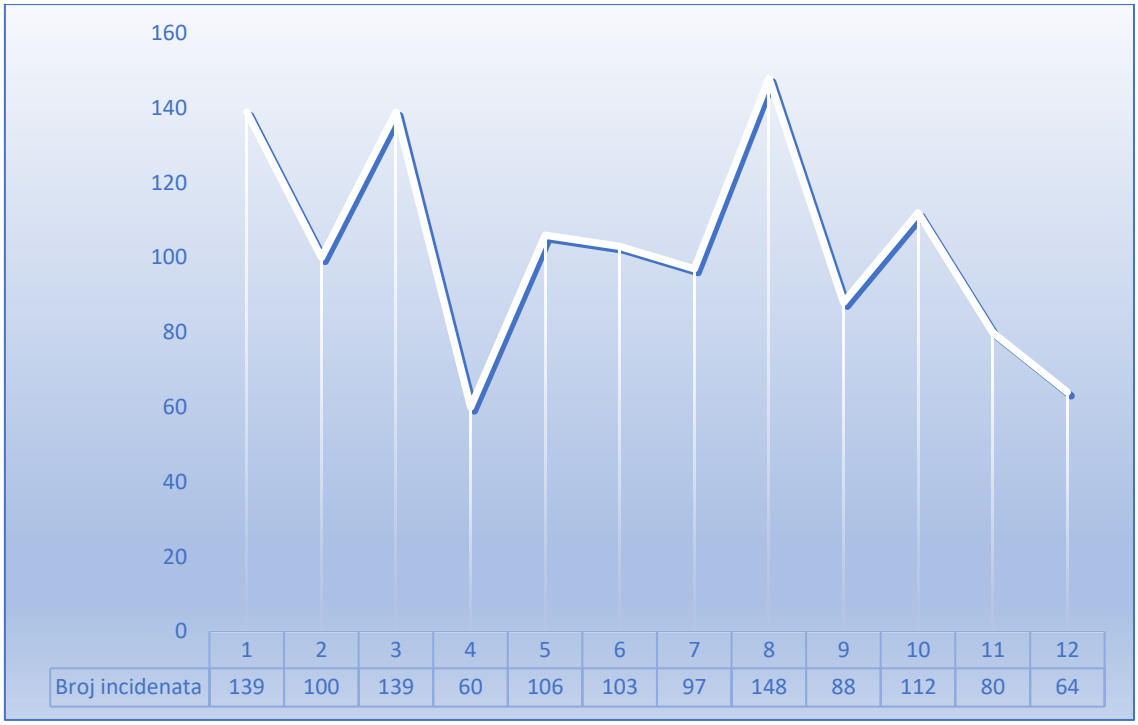


Raspodjela incidenata po tipu u 2023. godini

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 2023. 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 2023. godini

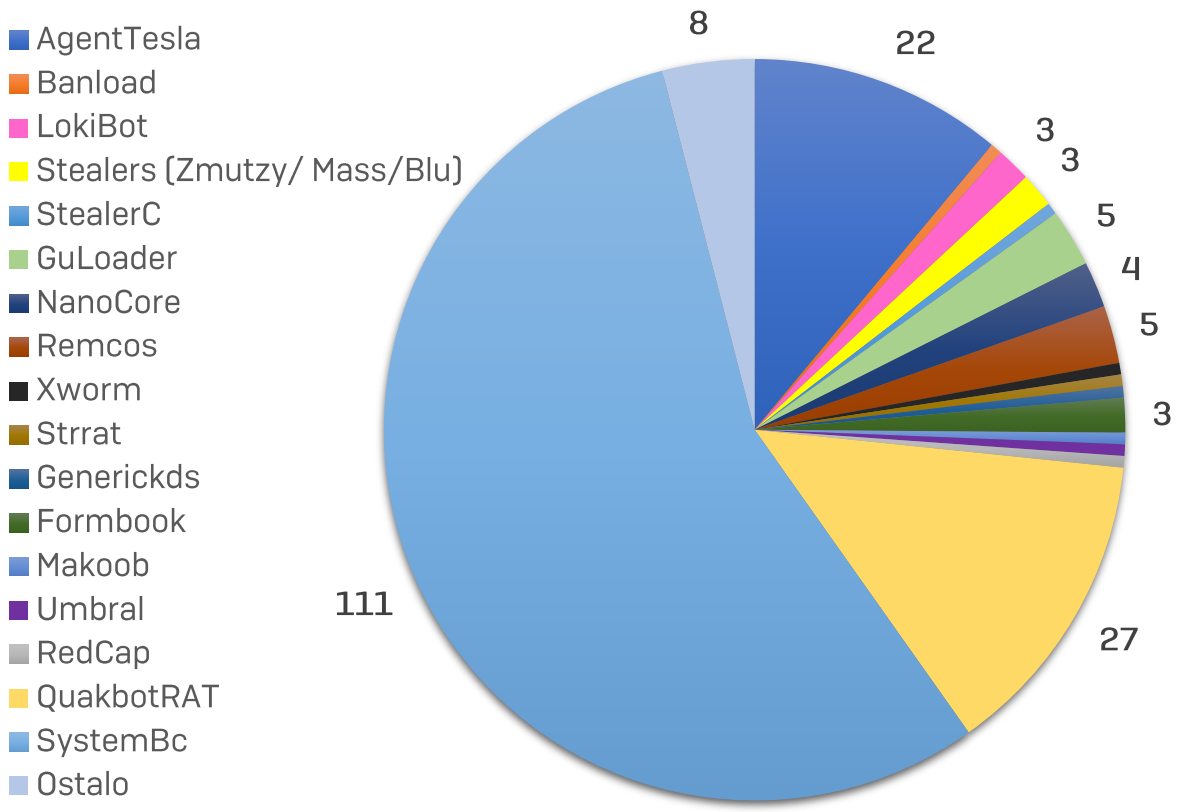
Na grafičkom prikazu vidljiva su tri skoka broja incidenata: u siječnju, ožujku i kolovozu. Prvi skok u siječnju je zabilježen zbog povećanog broja phishing incidenata iz domene financijskog sektora. Tematike phishing kampanja uključivale su prelazak na euro, usluge mobilnog/digitalnog/internet bankarstva te blokiranje računa i kartica zbog sigurnosnih mehanizama i mjera zaštite sustava.

Razlozi povećanog broja incidenata u ožujku bili su phishing kampanja na temu povrata poreza te scam kampanja. U scam kampanjama napadač se predstavljao kao visokopozicionirana osoba u policiji te pokušao zastrašiti potencijalnu žrtvu navodeći ju da odgovori na priloženi sudski poziv upućen zbog djela kibernetičkog kriminala, nakon čega bi slijedila iznuda financijske prirode.

Povećan broj incidenata zabilježen je i u kolovozu zbog phishing kampanja te sustava zaraženih zlonamjernim kôdom. Radilo se o hibridnim phishing kampanjama koje su ciljale poslovne korisnike banaka, prilikom kojih su korištene i smishing tehnike, uz vishing i klasični phishing putem elektroničke pošte.

2.4. Vrste malvera

U 2023. godini detektirano je oko 200 računala zaraženih malverom. Od tog broja 111 računala je zaraženo SystemBC malverima, 27 računala QuakBot Remote Access trojan malverima i 22 računala AgentTesla malverom. Većina malvera na zaraženim računalima bila je proširena putem elektroničke pošte ili preuzimanjem sumnjivih i neprovjerenih softvera.



Prikaz malvera po tipu

Analizirano je oko 200 malvera, od kojih je polovica zasebnih i pojedinačnih incidenata. Vrste malvera poput GuLoader, LokiBot i sl. često su u formatu NSIS installera. Broj malvera koji koriste NSIS značajno je porastao. S obzirom da je Windows platforma ona za koju se najviše malvera širilo u 2023. godini u Hrvatskoj, napadači su iskorištavali i prednosti sustava poput ugrađenog čitača .iso arhivskih datoteka - radi čega je porastao broj malvera koji se šire u .iso formatu. Veliki broj malvera i dalje dolazi u .docx, .xls i sličnim ekstenzijama te lažnim "pdf" datotekama gdje je prava ekstenzija .exe s PDF ikonom i često „-pdf" tekstom u imenu datoteke. Što se tiče obitelji malvera često se radi o

hibridima poput: Agenttesla s Makoob svojstvima ili Makoob s GuLoader svojstvima.

2.5. Registrirani botovi u Republici Hrvatskoj

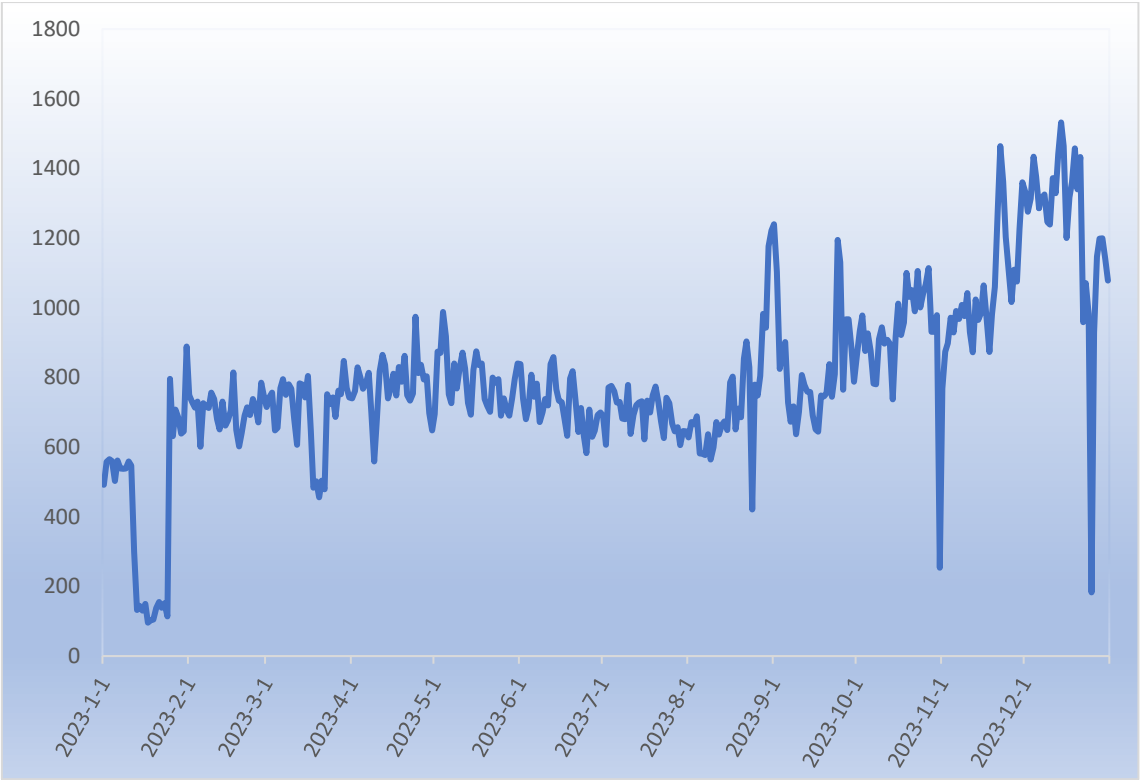
Nacionalni CERT primao je i statistički obrađivao podatke o *botovima* na računalima krajnjih korisnika. Podaci su prosljeđivani nadležnim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). U odnosu na 2022. godinu, u 2023. godini **značajno se povećao broj registriranih zaraženih računala u Hrvatskoj**. Zbroj zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2023. godine iznosi 138 676, što je **povećanje od 201,3 % u odnosu na 2022. 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 2023. godini, koji su bili proslijeđeni davateljima internetskih usluga.

Deset najčešće prijavljivanih *botova* u RH

Andromeda	**32590**
apk.hummer	**26634**
Mirai	**10245**
Gamut	**9174**
Adload	**9160**
socks5_systemz	**8751**
Vipersoftx	**7354**
Conficker	**4507**
pseudo_manuscrypt	**4015**
Flubot	**2920**



Broj zabilježenih *botova* po danima u 2023. godini

Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću oko **800 *botova* dnevno**, što je više od prošle godine. Srednja vrijednost broja *botova* po danu za 2023. godinu iznosila je 797,8 što je **povećanje za više od 496 botova** u odnosu na 2022. godinu. Navedeno povećanje broja botova se podudara sa povećanjem zabilježenih incidenata tipa sustav zaražen zlonamjernim kôdom.

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

Služba CARNET Abuse bavi se incidentom ako je izvor incidenta korisnik CARNET mreže (ustanova članica ili korisnik AAI@EduHr elektroničkog identiteta). Tijekom 2023. godine, služba CARNET **Abuse obradila je ukupno 1747 incidenata**. Broj incidenata se smanjio za gotovo 68% u odnosu na prošlogodišnjih 5411. Obzirom da se i ove godine većina incidenata (gotovo 90%) odnosi na povredu autorskih prava (distribucija datoteke putem BitTorrent protokola koja je zaštićena autorskim pravom), procjenjujemo da se broj incidenata smanjio zbog veće popularizacije streaming servisa multimedijskog sadržaja (npr. Netflix, HBO Max i sl.). 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. Suradnjom s ostalim pružateljima internetskih usluga (*eng. Internet Service Provider – ISP*) u Hrvatskoj, dio incidenata obrađuje se kod davatelja usluge koju pojedini korisnik koristi.

3. Značajni događaji po kvartalima

1. kvartal #378 incidenata #QRphishing #ESXiArgs #SupplyChain	Obrađeno je 378 računalno-sigurnosnih incidenata. Zabilježen je povećan broj phishing kampanja usmjerenih prema građanima i korisnicima hrvatskih banaka. Trendovi kampanja uključuju usluge mobilnog/digitalnog/internet bankarstva, blokiranje računa i kartica te sigurnosne mjere sustava. Napadačima je cilj krađa 2FA tokena/PIN-a/jednokratne zaporke, preuzimanje ovlasti nad računom i aplikacijom te krađa osobnih podataka i podataka o karticama. U pojedinim phishing kampanjama napadači se predstavljaju u ime državnih i javnih institucija Republike Hrvatske nudeći financijsku pomoć ili povrat novčanih sredstava. Po prvi puta primjećeno je korištenje phishing QR kôdova koji vode na stranice za krađu osobnih i bankovnih podataka, a forme imitiraju prijavu u mobilna bankarstva većih hrvatskih banaka. Objavljeno je upozorenje za korisnike banaka u suradnji s Hrvatskom udrugom banaka, kao i upozorenje za građane. Iz vanjskog izvora zaprimljene su informacije o ranjivosti VMware ESXi hipervizora koja se aktivno iskorištava za izvođenje ESXiArgs ransomware napada. Radi se o ranjivosti CVE-2021-21974 koja se iskorištava za izvršavanje proizvoljnog programskog kôda u sustavima (engl. *remote code execution – RCE*). Incident je prijavilo nekoliko visokoškolskih ustanova u Hrvatskoj, a dio ih je uspješno oporavio sustave pomoću sigurnosnih kopija. Naknadno su pronađeni potencijalno ranjivi sustavi te su pravovremeno obaviješteni. Objavljeno je upozorenje o ranjivosti te skripta za oporavak od ransomware napada.

	Detektirane su kompromitacije lanca opskrbe za 3CX Desktop aplikaciju. Zlonamjerna inačica aplikacije preuzima dodatne datoteke koje za cilj imaju krađu osjetljivih podataka, komunikaciju sa zlonamjernom infrastrukturom te u nekim slučajevima upravljanje kompromitiranim računalom. Zabilježene su zlonamjerne inačice (Windows: 18.12.407 i 18.12.416; Mac: 18.11.1213, 18.12.402, 18.12.407 i 18.12.416). Prikupljen je popis 3CX poslužitelja te su identificirani i obavješteni potencijalni korisnici zlonamjerne aplikacije. Objavljeno je upozorenje na stranicama Nacionalnog CERT-a.

2. kvartal #269 incidenata #hacktivizam #vishing #Fortinet	Obrađeno je 269 računalno-sigurnosnih incidenata. Zaprimljene su informacije o potencijalnim prijetnjama na informacijske sustave kritičnih sektora u Hrvatskoj. Haktivističke grupe prijetile su napadima uskraćivanjem usluga kritičnih sektora država članica EU. Proaktivno je pojačana mrežna propusnost i postavljena je antiDDoS zaštita na mreže ustanova. Dodatno, obaviještena su nacionalna sektorska tijela. Nije bilo zabilježenih napada na mrežnu infrastrukturu niti ustanove. Prvi puta zapaženo je korištenje *vishing* tehnike u phishing kampanjama koje ciljaju korisnike hrvatskih banaka. Radi se o phishing porukama koje sadrže phishing URL-ove s temom sprječavanja pranja novca. Nakon što potencijalna žrtva unese telefonski broj, zaprima poziv od „djelatnika" banke s lažiranog telefonskog broja banke koji tehnikama socijalnog inženjeringa traži dodatne podatke koji mu omogućuju prebacivanje novčanih sredstava na željeni račun. Kroz suradnju s Hrvatskom regulatornom agencijom za mrežne djelatnosti, Hrvatskom narodnom bankom i Ministarstvom unutarnjih poslova kontinuirano se radi na zaštiti korisnika od lažiranja telefonskih brojeva. Zaprimljene su informacije o kritičnoj ranjivosti Fortinet sustava pod oznakom CVE-2023-27997, koja potencijalnom udaljenom napadaču omogućuje izvršavanje proizvoljnog programskog kôda. Nacionalni CERT je poslao informacije o potencijalno ranjivim sustavima te preporuke o zakrpama nadležnim

	pružateljima internet usluga i usluga udomljavanja. Informacije o ranjivosti objavljene su na mrežnim stranicama Nacionalnog CERT-a.

3. kvartal #333 incidenta #sezona #smishing #investicijske prijevare #Ivanti #CARNET spearphishing #forenzika	Obrađeno je 333 računalno-sigurnosnih incidenata. Ususret ljetnoj sezoni, prijavljeno je nekoliko phishing napada na iznajmljivače apartmana. Napadači imitiraju zainteresirane goste i šalju phishing poruku s poveznicom na besplatne usluge za prijenos datoteka putem koje distribuiraju maliciozne privitke. Hibridne phishing kampanje u trećem kvartalu uključuju i korištenje smishing tehnike, uz vishing i klasični phishing putem elektroničke pošte. Najčešće se radi o tome da pošiljatelj koristi hrvatski broj ili lažirano alfanumeričko polje koje imitira različite usluge (kurirsku službu, poštu, sustav e-Građani ili banku). Primijećen je porast investicijskih prijevara. Radi se o prijevarama gdje se imitira poznata hrvatska tvrtka ili banka koja navodi potencijalnu žrtvu na ulaganje u zelene dionice, kriptovalute ili zlato, radi brze zarade. Nerijetko se na takvim stranicama lažiraju svjedočanstva poznatih ili političkih osoba. Izdana je zakrpa za ranjivost Ivanti Endpoint Manager Mobile (EPMM) paketa, koja omogućuje zaobilaženje autentifikacije, pod oznakom CVE-2023-35078. Obavješteni su vlasnici potencijalno ranjivih sustava te su objavljene informacije na mrežnim stranicama Nacionalnog CERT-a. Zbog završetka CARNET-ovog projekta e-Škole i medijske popraćenosti, primijećen je velik broj ciljanih (engl. *spear phishing*) kampanja usmjerenih prema CARNET-ovim korisnicima, upravi i zaposlenicima. Napadači šalju phishing poruke u kojima se nalazi phishing poveznica koja kopira izgled web stranica CARNET-ovih usluga. Phishing poruke dolaze kao obavijesti za Microsoft Office 365 usluge. Osim phishing prijevara, prijavljeni su i pokušaji poslovnih prijevara tipa CEO fraud.

4. kvartal

#256 incidenata

#ransomware

#ranjivosti

#WhatsApp

#shopping

Obrađeno je 256 računalno-sigurnosnih incidenata.

Zaprimljeno je nekoliko prijava zaraze različitim inačicama ransomwarea. Od međunarodne zajednice timova za obradu incidenata zaprimljene su informacije o sustavima zaraženim Mallox ransomwareom. Obavješteni su korisnici zaraženih sustava zbog mogućnosti dešifriranja sustava. Osim toga, zaprimljena je prijava zaraze poslužitelja 0XXX ransomwareom. Poslane se upute za potencijalno dešifriranje i najbolje sigurnosne prakse. Također, zaprimljena je prijava kompromitacije Lambda ransomwareom visokoškolske ustanove. Budući da se radi o relativno novoj inačici ransomwarea, trenutno ne postoji ključ za dešifriranje, ali je pružana savjetodavna podrška i forenzička analiza.

Osim ransomware napada, aktualne su ranjivosti različitih operacijskih sustava, uređaja i softvera. Poslane su obavijesti o potencijalno ranjivim Round Cube webmail instancama. Radi se o ranjivosti CVE-2023-5631 koja omogućuje napadačima udaljeno izvršavanje proizvoljnog JavaScript kôda u pregledniku žrtve slanjem posebno oblikovane poruke elektroničke pošte. Nadalje, poslane su obavijesti pružateljima usluga čiji su sustavi potencijalno ranjivi na ranjivost CVE-2023-46604 ActiveMQ instanci. Osim toga, poslane su obavijesti i za javno dostupne Unitronics PLC uređaje. Također, vlasnicima sustava proslijeđena su saznanja i o ranjivosti JetBrains TeamCity instance oznake CVE-2023-42793.

Zaprimljeno je nekoliko prijava hrvatskih građana za preuzimanje pristupa nad korisničkim računom jedne mobilne aplikacije. U suradnji s Hrvatskom regulatornom agencijom za mrežne djelatnosti, Agencijom za zaštitu osobnih podataka i Ministarstvom unutarnjih poslova zaključeno je kako se radilo o presretanju jednokratnog kôda kod SMS pružatelja treće strane.

Krajem godine, zbog perioda povećane kupovine (Crni petak, Cyber ponedjeljak, božićni blagdani) u suradnji s registrom .hr domene prijavljeno je i deaktivirano nekoliko

	lažnih web trgovina na .hr i .com.hr domenama, kao i lažnih web trgovina na stranim domenama.

4. Usluge CARNET-ovog Nacionalnog CERT-a

4.1. CERT SPAMBLOK

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

Praćenjem pokazatelja korištenja usluge vidljivo je da je dodatak postavljen na poslužiteljima e-pošte i mjesečno stavlja na crnu listu u prosjeku 39 jedinstvenih IP adresa i 4 jedinstvene domene, a broj korisničkih upita za pristigle poruke elektroničke pošte u mjesečnom prosjeku iznosi 935.317.

cert spamblok

4.2. CERT CVE

CERT CVE korisnicima omogućava pretplatu i praćenje informacija o poznatim ranjivostima unutar programskih paketa korištenijih operativnih sustava. Uz to, korisnicima omogućava brže pretraživanje poznatih ranjivosti prema specifičnim kriterijima kao što su proizvođač, CWE 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.

Početkom 2023. godine naziv usluge CERT EPSILON je promijenjen u CERT CVE. Izvršene su nadogradnje usluge: omogućeno je primanje obavijesti u tabličnom prikazu novih i starih vrijednosti pojedinog CVE-a kako bi se mogle pratiti promjene i dobivanje točnijih i bržih informacija o zadnjim ažuriranjima postojećih i dodavanja novih CVE oznaka.

Prema pokazateljima korištenja usluge u protekloj godini ukupan broj korisnika usluge je 184, a ukupan broj posjeta stranici je 6553.

cert cve

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

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

incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga.

Prema pokazateljima korištenja usluge u protekloj godini ukupan broj korisnika usluge je 267 iz 119 institucija.

4.4. Sigurnost CARNET usluga

Tijekom 2023. godine Služba za sigurnost usluga i infrastrukture CARNET-ovog Nacionalnog CERT-a provodila je sljedeće aktivnosti s ciljem povećanja razine sigurnosti CARNET-ovih usluga i infrastrukture.

- prikupljanje i analiza sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija i usluga CARNET-a;
- usluga izdavanja elektroničkih certifikata (TCS);
- provođenje odredaba Programa sigurnosti;
- uvođenje novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNET-a;
- redovita provjera ranjivosti (eng. *Vulnerability Scanning*) ustanova članica CARNET mreže;
- analiza stanja sigurnosti CARNET-ovog IP adresnog prostora ovisno o ugrozama;
- analiza stanja sigurnosti CARNET ustanove radi unaprjeđenja sigurnosti;

Tijekom 2023. godine Nacionalni CERT je u sklopu tih aktivnosti:

- provodio penetracijska testiranja (19) važnih CARNET-ovih usluga u sklopu implementacije Programa sigurnosti u CARNET-ove poslovne procese;
- provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET;
- 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 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 ju 62 ustanove iz sustava obrazovanja, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže. U 2023. godini provedeno je ukupno 81 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 2023. godini izdano je ukupno 2554 certifikata: 2501 poslužiteljskih certifikata, 52 klijentska i 1 code signing certifikat.

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 CyberSOPEx 2023

U utorak, 7. studenog 2023. godine održana je kibernetička vježba "Cyber SOPEx" s ciljem poboljšanja suradnje između CSIRT-ova (eng. Computer Security Incident Response Team). Vježba se održala uz koordinaciju ENISA-e (Agencije Europske unije za kibernetičku sigurnost) koja je pratila provođenje standardnih operativnih procedura CSIRTs Network zajednice.

Više od 28 europskih timova, uključujući Nacionalni CERT, sudjelovalo je u vježbi čiji se scenarij odvijao oko kibernetičkih napada u energetskom sektoru. Vježbom su se, osim suradnje, poticale kreativne ideje.

"Cyber SOPEx" jedna je od ENISA-inih vježbi kojima je fokus na podizanju svijesti o pojedinoj situaciji, dijeljenju informacija, razumijevanju uloga i odgovornosti unutar tima te korištenje alata potrebnih za uspješno rješavanje incidenata. Dugogodišnji cilj ovog projekta je poboljšanje operativne suradnje u području kibernetičke sigurnosti unutar Europske unije.

Mreža europskih timova za obradu računalno-sigurnosnih incidenta (CSIRTs Network) nastala je temeljem direktive o mrežnoj i informacijskoj sigurnosti (NIS direktiva) koju je donijela Europska unija 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.

5.2. Vježba Cyber Coalition 2023

Hrvatska akademska i istraživačka mreža - CARNET i Nacionalni CERT aktivno su sudjelovali u šesnaestoj po redu NATO vježbi zaštite NATO-a i nacionalnih računalnih sustava pod nazivom „Cyber Coalition 2023". Cilj vježbe je osnažiti koordinaciju i suradnju između NATO Saveza i njegovih članica, te poboljšati mogućnosti odvraćanja, obrane i suzbijanja prijetnji u i kroz kibernetički prostor. „Cyber Coalition 2023" najveća je NATO vježba u području kibernetičke obrane. Organizirana je od strane Savezničkog zapovjedništva za transformacije (ACT), a održavala se od 27. studenog do 01. prosinca na više desetaka lokacija u zemljama sudionicama. Vježba je okupila više od 1300 sudionika iz 35 zemalja članica NATO-a i partnerskih zemalja, akademske zajednice i industrije. Sudionici su uključivali najnovijeg saveznika Finsku, zemlje partnere Švedsku, Gruziju, Irsku, Japan, Južnu Koreju, Švicarsku, Ukrajinu, kao i Europsku uniju.

Scenariji na vježbi simulirali su ugroze iz stvarnog života kao što su napadi na prometnu infrastrukturu i financijski sektor, programe i sredstva NATO-a i Saveznika tijekom vojnih operacija.
CARNET i Nacionalni CERT su u vježbi sudjelovali u dijelu scenarija svojih nadležnosti, u tehničkom dijelu, pravnom scenariju i kriznoj komunikaciji te su koordinirali sudjelovanje igrača i igračica iz privatnog sektora i akademske zajednice. Osim otkrivanja incidenata, provedbe obrambene kibernetičke operacije i oporavka sustava, čime se bavila tehnička obučna skupina, hrvatska provedba uključivala je također operativnu i pravnu obučnu skupinu. Operativna

skupina imala je zadaću koordinacije i osiguranja provedbe vojne operacije u uvjetima degradirane slobode djelovanja u kibernetičkom prostoru, dok je pravna skupina osiguravala donošenje odluka u skladu s međunarodnim pravom i praksom te poduzimanje pravnih mjera protiv počinitelja. Ove je godine po prvi put nacionalno provježbana skupina za krizno komuniciranje.
Republika Hrvatska u vježbi sudjeluje od 2009. godine kao promatrač, a od 2013. kao aktivni sudionik vježbe. Od 2015. godine vježbi su se pridružili i predstavnici iz privatnog sektora i akademske zajednice. Iz privatnog sektora u vježbi su sudjelovale tvrtke: APIS IT do.o.o., ATO inženjering d.o.o., CyberArrange Security Solutions j.do.o., NEP-054 obrt za usluge savjetovanja, OsijekOffset Concepts obrt za programiranje, Infigo IS d.o.o., Infobip d.o.o. , Insig2 d.o.o., Microsoft Hrvatska d.o.o., SPAN d.d. i Utilis 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, Pravni fakultet Zagreb, 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.

NORTH ATLANTIC TREATY ORGANIZATION

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. Na sastancima se predstavljaju

rezultati radnih grupa koje su oformljene unutar CSIRT mreže s ciljem unaprjeđenja suradnje, komunikacije i razmjene informacija među CSIRT-ovima Europske unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a te razmjenu znanja i razvoj alata koji se koriste u CSIRT zajednici. Osim ranije spomenutog, na sastancima se redovito izvještava o aktivnostima ENISA-e, 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.

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

6.1. Sporazum o poslovnoj suradnji s MUP-om

U 2023. 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. Suradnja s FER-om

CARNET-ov Nacionalni CERT nastavlja suradnju s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu, Laboratorijem za sustave i signale (LSS) Zavoda za elektroničke sustave i obradu informacija FER-a. Tijekom 2023. godine objavljena su dva dokumenta na teme iz područja kibernetičke sigurnosti. Dokumenti „Sigurnosni rizici pohrane lozinki u preglednike“ i „Zlouporaba umjetne inteligencije“ namijenjeni su svima koji žele znati više o kibernetičkoj sigurnosti. Posebno valja izdvojiti organizaciju i provedbu četvrtog CTF natjecanja za srednjoškolce pod nazivom “H4cknite” tijekom listopada u sklopu aktivnosti Europskog mjeseca kibernetičke sigurnosti. Za potrebe natjecanja razvijeni su vrlo zanimljivi i izazovni sadržaji. Natjecanje i platforma Hacknite, na kojoj se nalaze zadaci i edukativni materijali, pružaju priliku svim zainteresiranim učenicima za učenje o kibernetičkoj sigurnosti. Više o samom natjecanju i platformi u poglavlju 6.7.

6.3. Sudjelovanje u radu tijela iz Nacionalne strategije kibernetičke sigurnosti

Tijekom 2023. 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

Tijekom 2023. 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. Međusektorska suradnja vrlo je važna u borbi protiv kibernetičkih incidenata. Sektor bankarstva jedan je od pet sektora za koji je Nacionalni CERT nadležni CSIRT sukladno Zakonu. Na sastancima se izvještava o trendovima i eventualnim aktualnim ugrozama u području kibernetičke sigurnosti, a zainteresirane banke mogu se obraditi Nacionalnom CERT-u kako bi zaprimale tjedne izvještaje o ranjivim servisima.

HRVATSKA UDRUGA BANAKA
CROATIAN BANKING ASSOCIATION

6.6. Obilježavanje Europskog mjeseca kibernetičke sigurnosti (ECSM)

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

Tema prošlogodišnje kampanje bila je socijalni inženjering koji podrazumijeva manipulaciju žrtve kako bi se od nje ostvarila neka korist. U socijalni inženjering spada i phishing, a budući da u statistici naših obrađenih incidenata phishing čini 49% važno je građanima pojasniti ovu prijetnju i načine zaštite od nje.

U sklopu ECSM-a surađivali smo na izradi i provedbi GÉANT-ove "*Become a Cyber Hero*" kampanje. U sklopu GÉANT kampanje snimljen je i animirani serijal "Cybercrime for Newbies" u kojem Granny Smith #85 opisuje svoju avanturu pokušaja napada izvršenih pomoću socijalnog inženjeringa i pretraživanja javno dostupnih podataka.

Za vrijeme ECSM kampanje, objavljeni su brojni savjeti za prepoznavanje i zaštitu od socijanog inženjeringa te su održana predavanja i webinari na teme kibernetičke sigurnosti.

6.7. H4CKNITE– četvrto CTF natjecanje za srednjoškolce

Četvrto izdanje hrvatskog CTF natjecanja za srednjoškolce H4CKNITE provedeno je od 13. do 15. listopada 2023. 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 315 učenika u 63 srednjoškolska tima iz 40 srednjih škola. Pobjednički tim bio je BrownBird Team iz Tehničke škole Ruđera Boškovića Zagreb. Po uzoru na prošlogodišnje pobjednike, članovi BrownBird Teama, sastavili su upute za rješavanje zadataka s natjecanja koje se mogu pronaći na Hacknite platformi.

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

Hrvatski nacionalni tim CRØnquerors, sastavljen je od pet juniora i pet seniora, sudjelovao je na European Cyber Security Challenge-u (ECSC) održanom u norveškom Hamaru od 24. do 27. listopada. ECSC je godišnje europsko natjecanje koje okuplja mlade talente iz cijele Europe kako bi se zabavili i natjecali u područjima kibernetičke sigurnosti. Deset natjecatelja praćena trenerom i voditeljem tima iskušali su svoje vještine u CTF-u (Jeopardy Style i Attack and Defense) obliku natjecanja.

6.8. Dan sigurnijeg interneta 2023.

Nacionalni CERT obilježio je Dan sigurnijeg interneta sudjelujući na konferenciji Centra za sigurniji internet i videokonferenciji "Potraga za boljim internetom" s ciljem podizanja kompetencija za sigurno korištenje interneta i ostalih digitalnih tehnologija.

Cjelodnevna video konferencija „Potraga za boljim internetom" provedena je u suradnji s Udrugom „Suradnici u učenju" i drugim partnerima obuhvatila je teme sigurnosti na internetu, zaštite virtualnog identiteta i osobnih podataka, utjecaju digitalnih medija na mentalno zdravlje mladih, elektroničkom nasilju, pravima djece u digitalnom okruženju, 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 jubilarnom 10. kampanjom podizanja svijesti povodom Europskog mjeseca kibernetičke sigurnosti te s HACKNITE natjecanjem za srednje škole.

Centar za sigurniji Internet je u suradnji s A1 Hrvatska u OŠ Središće u Zagrebu održao deveti Dan sigurnijeg interneta u Hrvatskoj. Uz panel raspravu održan je stručni skup pod nazivom "Koja je cijena jednog LAJKA?" na kojem je Nacionalni CERT predstavio svoje aktivnosti u području zaštite od internetskih ugroza i edukacija iz područja kibernetičke sigurnosti.

Pridružili smo se obilježavanju Dana sigurnijeg interneta u Osnovnoj školi Rapska u organizaciji HAKOM-a gdje smo učenike upoznali s radom Nacionalnog CERT-a, ukazali na najčešće prijetnje na internetu i pričali o važnosti brige o digitalnom tragu i održavanju kibernetičke higijene.

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, 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. Velik interes medija zamijećen je u praćenju tema iz područja razvoja i primjene umjetne inteligencije.

Konferencije, edukacije i mrežni seminari

Predstavnici Nacionalnog CERT-a sudjelovali su na brojnim događanjima na kojima su predstavljene razne teme iz područja kibernetičke sigurnosti od kojih izdvajamo konferencije povodom Dana sigurnijeg interneta, konferencija u okviru projekta SURF and SOUND, videokonferencija s OŠ Stjepana Radića Brestovec Orehovečki, konferencija Strategija urbane sigurnosti Grada Zagreba, stručni skupovi Agencije za odgoj i obrazovanje, konferencija „Konferencija država Jugoistočne Europe o kibernetičkom kriminalu" te konferencije za CARNET-ove korisnike. Pomoćnica ravnatelja za Nacionalni CERT sudjelovala je na panel raspravi o budućem razvoju ekosustava kibernetičke sigurnosti u Hrvatskoj i ključnim promjenama koje nas očekuju uslijed donošenja NIS2 Direktive i drugih inicijativa Europske unije u području informacijske sigurnosti i koordiniranih zajedničkih akcija i projekata.

Nacionalni CERT je tijekom 2023. godine održao brojna predavanja za različite ciljne skupine od kojih bismo izdvojili predavanja u osnovnim školama, edukacije nastavnika te edukacije za CARNET-ove zaposlenike radi jačanja otpornosti na kibernetičke prijetnje.

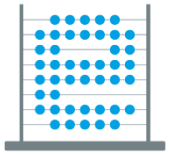
Informirali smo javnost putem web sjedišta Nacionalnog CERT-a (https://www.cert.hr/) kojeg je 2023. godine posjetilo ukupno 185.536 posjetitelja te putem društvenih mreža Facebook (2212 pratitelja) i Twitter (1485 pratitelja).

7. Projekti

Nacionalni CERT je sudjelovao u provedbi pet projekata sufinancirana sredstvima Europske unije: "e-Škole: Cjelovita informatizacija procesa poslovanja škola i nastavnih procesa u svrhu stvaranja digitalno zrelih škola za 21. stoljeće", Podrška primjeni digitalnih tehnologija u obrazovanju – BrAIn, Hrvatska kvantna komunikacijska infrastruktura – CroQCI, e-Sveučilišta i kao partner na projektima CEKOM (Centar kompetencija za kibernetičku sigurnost upravljačkih sustava).

7.1. e-Škole

U 2023. 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.



e-Škole

7.2. Podrška primjeni digitalnih tehnologija u obrazovanju - BrAIn

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

Elementi projekta:

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

Pametna kibernetička sigurnost obuhvatit će aktivnosti: uporaba umjetne inteligencije za automatizaciju internih procesa automatizacije obrade kibernetičkih incidenata, usklađivanje procesa s europskom i nacionalnom

regulativom te unapređivanje sustava za ranu detekciju ranjivosti mogućih incidenata kao i primjenu umjetne inteligencije u izradi programa za podizanje svijesti o kibernetičkoj sigurnosti.

7.3. Hrvatska kvantna komunikacijska infrastruktura - CroQCI

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

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

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

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

7.4. e-Sveučilišta

CARNET provodi projekt e-Sveučilišta s ciljem digitalne preobrazbe visokog obrazovanja u Republici Hrvatskoj poboljšanjem digitalne nastavne infrastrukture, uvođenjem digitalnih nastavnih alata te osnaživanjem digitalnih kompetencija nastavnika za poučavanje u digitalnom okruženju. Projekt traje od ožujka 2022. do prosinca 2025. godine. U ustanovama visokog obrazovanja izgradit će se i/ili nadograditi mrežna i/ili računalna infrastruktura. Ustanove će dobiti napredno upravljanje mrežom sa sigurnosnom komponentom, mogućnost korištenja naprednih mrežnih servisa s osiguranim kapacitetom i stabilnosti veze. Ustanove će dobiti i popratne servise i alate kao i digitalnu nastavnu opremu. Kroz sve segmente opremanja fokus će biti na sigurnosnoj komponenti.

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

7.5. CEKOM

Nacionalni CERT je sudjelovao u projektu Centar kompetencija za kibernetičku sigurnost upravljačkih sustava – CEKOM. Cilj trogodišnjeg projekta bio 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 bila 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., sudjelovao je kao partner na projektu.

7.6. Cybersecurity Ninja

CYBERSECURITY NINJA – Educating Young People and Their Parents on How to Fight Cybersecurity Challenges, je projekt financiran od strane Vlade Sjedinjenih Američkih Država, U.S. Department of State, Bureau of Educational and Cultural Affairs uz koordinaciju s Meridian International centrom. Ciljeve projekta smislila je i provela voditeljica Službe za obradu incidenata u Nacionalnom CERT-u, ujedno alumna IVLP (International Visitors Leadership Program) razmjene, dok je CARNET u projektu sudjelovao kao partner.

U sklopu projekta provedeno je 12 radionica u 5 hrvatskih gradova (Rijeka, Split, Osijek, Varaždin i Zagreb), educirane su 384 osobe, osmišljena je i u 500 primjeraka otiskana edukativna brošura „Cybersecurity Ninja“. Završno događanje obilježeno je raspravom o zaštiti djece i ulaganju u buduće stručnjake iz područja kibernetičke sigurnosti na okruglom stolu stručnjaka iz područja kibernetičke sigurnosti. Projekt je omogućio stvaranje novih budućih suradnji u području širenja svijesti o kibernetičkoj sigurnosti djece i prijetnjama s kojima se svakodnevno susreću.

8. O Nacionalnom CERT-u

Nacionalni CERT (CERT.hr) je sektor Hrvatske akademske i istraživačke mreže – CARNET.

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.

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.

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
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.
Malver	Zlonamjerni softver namijenjen infiltraciji računala bez znanja njegovog vlasnika, odnosno korisnika.
Malver URL	Poveznica do zlonamjernog sadržaja na kompromitiranom web sjedištu.
Payload	Malver koji akter prijetnje namjerava isporučiti žrtvi. Na primjer, ako je kibernetički kriminalac poslao e-poruku sa zlonamjernom makronaredbom kao privitkom, a žrtva se zarazi ransomwareom, tada je ransomware korisni teret (a ne e-pošta ili dokument).
Phishing	Pokušaj navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala.
Phishing URL	Poveznica do lažne Internet stranice na kompromitiranom web sjedištu ili sjedištu registriranom u svrhu krađe povjerljivih podataka.

Poslovna prijevara	Napadi kod kojih napadač lažnim predstavljanjem pokušava steći ili stekne financijsku korist od ciljanog poslovnog korisnika. Jedan on najčešćih oblika ovakvih napada su tzv. „CEO fraud“ ili „BEC“ (Business Email Compromise).
Ransomware	Naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala.
Scam	Pokušaj navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte). Najpoznatiji oblik je „nigerian scam“ ili „419 fraud“.
Smishing	Phishing putem sms-a.
Sniffing	Sniffing podrazumijeva neovlašteno presretanje mrežnog prometa.
Spam	Neželjena elektronička poruka reklamnog sadržaja.
Spam URL	*Spam* sadržaj na kompromitiranom *web* sjedištu koji se distribuira kroz *spam* poruke.
Spyware	Vrsta malicioznog programa čija je namjena sakupljanje informacija te preuzimanje kontrole rada na računalu korisnika bez njegova znanja ili dozvole.
SQL injection napadi	Napad umetanjem SQL kôda koji iskorištava ranjivosti na sloju baze podataka.
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

- računalno-sigurnosne incidente prijavite na incident@cert.hr

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

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

Nacionalni CERT u brojkama	
Poslužiteljski elektronički certifikati	2.501
Klijentski elektronički certifikati	52
Broj pretplata na preporuke	184
Broj registriranih botova	138.676
Obrađenih sigurnosnih incidenata	1.236
Analiza prijavljenih sigurnosnih događaja u CARNET mreži	53
Provjera sigurnosti CARNET aplikacija, komponenata i usluga	19
Certificiranje CARNET aplikacija koje pristupaju sustavu „e-Matica“	2
Objavljene novosti	193
Provjera ranjivosti	81
Broj objavljenih upozorenja	11
Broj objavljenih dokumenata	2
Posjeta portalu www.cert.hr	185.536
Broj pratitelja na Facebook @CERT.hr	2.212
Broj pratitelja na Twitter @HRCERT	1.485

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)