CERT.hr
surfaj sigurnije

Godišnji izvještaj Nacionalnog CERT-a za 2018. godinu

Sadržaj

1 Usluge Nacionalnog CERT-a

Nacionalni CERT (eng. *Computer Emergency Response Team*) odjel je Hrvatske akademske i istraživačke mreže – CARNET, čiji je osnovni zadatak obrada incidenata na internetu odnosno očuvanje kibernetičke sigurnosti u Republici Hrvatskoj. Nacionalni CERT bavi se 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 CERT ZSIS (CERT Zavoda za sigurnost informacijskih sustava).

Nacionalni CERT osnovan je 30. listopada 2007. godine kada je Upravno vijeće CARNET-a prema obvezama Zakona o informacijskoj sigurnosti donijelo izmjene statuta kojima je uspostavljen Odjel za Nacionalni CERT. Do tada, jedini CERT u Republici Hrvatskoj bio je CARNET CERT koji je osnovan 1996. godine. 2013. godine Nacionalni CERT preuzima sve poslove koje je obavljao CARNET CERT. Tako je CARNET omogućio bolju brigu o sigurnosti javnih informacijskih sustava kroz djelatnost Nacionalnog CERT-a te pružio kvalitetniju uslugu korisnicima u sustavu znanosti i obrazovanja kroz aktivnosti tadašnjeg CARNET-ovog Odjela za računalnu sigurnost (2016. godine i taj je odjel pripojen Odjelu za Nacionalni CERT). Nakon ustrojstva Nacionalnog CERT-a započinje uspostava hijerarhijski ustrojene infrastrukture CERT timova koja je nužna za preventivno djelovanje i učinkovitu koordinaciju pri rješavanju računalno-sigurnosnih incidenata vezanih uz informacijsko-komunikacijske sustave.

Tijekom 2018. godine Nacionalni CERT provodio je svoje proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenata i smanjenja šteta pri njihovom nastanku.

1.1. Proaktivne mjere

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

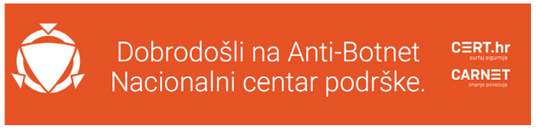
- svakodnevno izdavanje sigurnosnih preporuka za najpopularnije operativne sustave;
- izdavanje i objavljivanje dokumenata o temama iz područja kibernetičke sigurnosti;
- izdavanje i objavljivanje tehničkih informacija o sigurnosnim alatima;
- praćenje i objavljivanje novosti u vezi kibernetičke sigurnosti;
- provjera ranjivosti ustanova članica CARNET mreže;
- provjera ranjivosti drugih korisnika u Republici Hrvatskoj, prema dogovoru;
- informiranje javnosti putem portala www.antibot.hr s ciljem suzbijanja botova;
- sudjelovanje u televizijskim i radijskim emisijama;
- sudjelovanje na predavanjima u sklopu konferencija i radionica;
- održavanje predavanja i webinara o sigurnosti na internetu.

Broj izvršenih proaktivnih mjera u 2018. godini

Alati	10
Dokumenti	13
Novosti	139
Ukupno preporuka	3 070
Broj provjera ranjivosti	226
Broj izdanih elektroničkih certifikata	697

Portal antibot.hr

Nacionalni centar potpore Antibot krajnjim korisnicima omogućuje bolju detekciju i uklanjanje zlonamjernih programa s njihovih računala. U 2018. godini portal Antibot posjetilo je 55 064 korisnika.



EU-Cleaner

U suradnji s tehnološkim partnerima Avira, Gdata i SurfRight, **Antibot** nudi mogućnost besplatnog preuzimanja alata EU Cleaner koji pomaže pri laganom i brzom uklanjanju zlonamjernih programa.

Ransomware

U posebnoj kategoriji **Ransomware** mogu se pronaći sve bitne informacije i savjeti vezani uz ransomware, kao i poveznice na alate za dešifriranje datoteka u slučaju otkrivanja ključa.

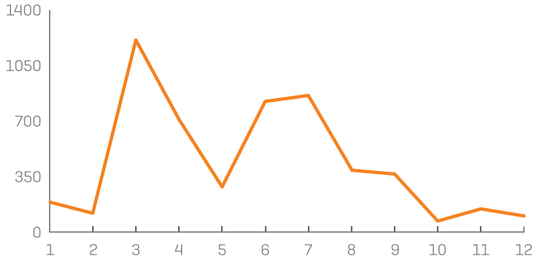
Alati

Kategorija **Alati** na jednom mjestu nudi vrlo koristan pregled antivirusnih programa u besplatnoj ili naplatnoj inačici, dodataka koji nadopunjavaju web preglednike s ciljem povećanja sigurnosti računala te poveznica za preuzimanje istih, preporuka za vanjske sigurnosne provjere, poput provjera phishing stranica

ili zlonamjernih programa, te korisnih alata koji krajnjem korisniku mogu poslužiti u svakodnevnom korištenju računala, tableta ili pametnih telefona (donosi poveznice za preuzimanje različitih alata kao što su alati za izradu sigurnosnih kopija, spremanje lozinki i mnogi drugih). Pomoću senzora instaliranih unutar većih ISP-eva i fakulteta u Hrvatskoj, CARNET (Nacionalni CERT) može detektirati aktivne zlonamjerne domene kojima pristupaju zaražena korisnička računala.

Spam

Također se prikuplja i analizira neželjena elektronička pošta (eng. *spam*) koja može sadržavati zlonamjerne URL-ove ili privitke. Takva elektronička pošta najčešće je prvi korak pri infekciji računala krajnjeg korisnika. Rezultati koji detaljno prikazuju neželjene elektroničke poruke (spam) sa zlonamjernim sadržajem nalaze se pod kategorijom **Spam**.



*Zlonamjerni sadržaj detektiran **spamtrap** senzorom u 2018. godini.*

Provjera ranjivosti

Nacionalni CERT nudi uslugu redovite provjere ranjivosti ustanova članica CARNET mreže. Redovita provjera ranjivosti obavlja se periodički svaka tri mjeseca, a rezultati se šalju odgovornim osobama ustanova u obliku izvještaja koji sadrži listu pronađenih sigurnosnih propusta i upute za njihovo rješavanje.

Uslugu redovite provjere ranjivosti koristi 57 ustanova iz sustava prosvjete, visokog obrazovanja, kulture te neka državna tijela unutar CARNET mreže.

Stručnjaci Nacionalnog CERT-a provode i masovne provjere ranjivosti CARNET mreže. Automatiziranu masovnu provjeru velikog broja ustanova u kratkom vremenu omogućava softverska komponenta SPORt (sustav za pohranu, obradu i preuzimanje rezultata) razvijena u Nacionalnom CERT-u. **SPORt** omogućava dostavu izvještaja o pronađenim ranjivostima putem web sjedišta uz prethodnu prijavu administratora na ustanovi. Rezultati obavljenih provjera daju uvid u sigurnosno stanje CARNET mreže te smjernice za daljnje planiranje s ciljem smanjenja broja ranjivosti.

1.2. Reaktivne mjere

Reaktivnim mjerama djeluje se na incidente u Republici Hrvatskoj te na druge događaje koji mogu ugroziti kibernetičku sigurnost javnih informacijskih sustava u Republici Hrvatskoj. Neke od reaktivnih mjera koje provodi Nacionalni CERT su::

- obrada incidenata (svi korisnici u Hrvatskoj, uključujući korisnike CARNET-a);;
- 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.

Statistički podaci provedenih reaktivnih mjera u 2018. godini nalaze se u **poglavlju 5: Stanje računalnih incidenata i statistike.**

DNSBL

Uz postojeći Spamtrap sustav koji uspješno prikuplja i analizira neželjenu poštu, Nacionalni CERT je razvio i sustav DNSBL (eng. *domain name server blacklist*) ili RBL sustav (eng. *real time blacklist*) koji je prvenstveno namijenjen korisnicima u Hrvatskoj i omogućava im smanjivanje količine neželjene pošte. Svrha DNSBL liste je smanjivanje količine neželjene pošte koju šalju pošiljatelji iz Hrvatske i regije (tzv. spameri), a koji često nisu obuhvaćeni poznatim globalnim listama. DNSBL lista nije zamjena za poznate liste kao što su Spamhaus, SpamCop, Sorbs i sl. Usluga je korisnicima dostupna od svibnja 2018. godine, a razvijena je u sklopu projekta GrowCERT.

1.3. Sigurnost usluga

Tijekom 2018. godine provodile su se aktivnosti unutar CARNET-ovog odjela za Nacionalni CERT koje su za cilj imale povećanje razine sigurnosti CARNET-ovih usluga, računalnih sustava i cjelokupne mreže, a to su:

- prikupljanje i analiza sigurnosnih događaja u CARNET mreži;
- provjera sigurnosti aplikacija, komponenata i usluga CARNET-a;
- provjera ranjivosti mrežnih uređaja u jezgri CARNET mreže;
- usluga izdavanja elektroničkih certifikata (TCS-om);
- provođenje odredaba Programa sigurnosti;
- uvođenje novih tehnologija sa sigurnosnog aspekta u informacijski sustav CARNET-a.

Tijekom 2018. godine Nacionalni CERT je u sklopu tih aktivnosti:

- izdao 605 poslužiteljskih certifikata, od toga 57 Extended Validation (EV) te 35 klijentskih certifikata;
- provodio penetracijska testiranja važnih CARNET-ovih usluga u sklopu implementacije programa sigurnosti u CARNET-ovim poslovnim procesima;
- provjeravao sigurnost usluga razvijenih u CARNET-u ili za CARNET;
- certificirao aplikacije koje pristupaju sustavu "e-Matica";
- sudjelovao u projektu GEANT 4-2 na aktivnosti SA2/T1;
- pružao potporu sigurnosnom dijelu projekta "e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)".

2 Suradnja i djelovanje Nacionalnog CERT-a na međunarodnoj razini

Pored institucija **EU-a** i **NATO-a**, Nacionalni CERT surađuje s međunarodnim udruženjima CERT-ova **FIRST** (eng. *Forum of Incident Response and Security Teams*) i **TI** (eng. *Trusted Introducer*), čiji je akreditirani član.

2.1. Vježba u Cyber SOPEx 2018

Agencija Europske unije za mrežnu i informacijsku sigurnost, ENISA (eng. *European Network and Information Security Agency*), 30. siječnja 2018. godine organizirala je kibernetičku vježbu "Cyber SOPEx" s ciljem poboljšanja suradnje između CSIRT-ova (eng. *Computer Security Incident Response Team*). Ovo je bila prva vježba takvog tipa. Preko 70 specijalista iz europskih CSIRT-ova i CERT-ova, uključujući Nacionalni CERT, sudjelovalo je u vježbi čiji se scenarij temeljio na kibernetičkim napadima na pomorski sektor. Vježbom se, osim suradnje, poticao i kreativni pristup rješavanju računalno-sigurnosnih incidenata. "Cyber SOPEx" prvi je korak u seriji ENISA-inih vježbi kojima je fokus na podizanju svijesti o pojedinoj situaciji, dijeljenju informacija, razumijevanju uloga i odgovornosti unutar tima te korištenju alata potrebnih za uspješno rješavanje incidenata. Dugogodišnji cilj ovog projekta je poboljšanje operativne suradnje u području kibernetičke sigurnosti unutar Europske unije.

2.2. Vježba Cyber Europe 2018

Nacionalni CERT je i 2018. godine sudjelovao u međunarodnoj vježbi Cyber Europe 2018 koju je organizirala ENISA u suradnji s tijelima i agencijama iz područja kibernetičke sigurnosti iz cijele Europe. Čak 900 europskih stručnjaka iz područja kibernetičke sigurnosti iz 30 zemalja tijekom vježbe koja se održavala 6. i 7. lipnja 2018. godine bilo je suočeno s intenzivnim scenarijem računalno-sigurnosnog incidenta u zračnoj luci. Ovu dvodnevnu vježbu ENISA je organizirala u svom sjedištu u Ateni (Grčka), a sudionici su ostali na svojim uobičajenim radnim mjestima ili su se okupili u skupinama za djelovanje u kriznim situacijama. Scenarij je sadržavao tehničke i netehničke probleme temeljene na stvarnim iskustvima za čije rješavanje je bila potrebna mrežna analiza i analiza zlonamjernog softvera, forenzika i steganografija. Incidenti u scenariju osmišljeni su tako da prerastu u krizu na svim mogućim razinama: organizacijskoj, lokalnoj, nacionalnoj i europskoj. Cilj vježbe CE2018 bio je omogućiti europskoj zajednici u području kibernetičke sigurnosti daljnje jačanje njenih sposobnosti za prepoznavanje i rješavanje prijetnji velikog razmjera te omogućiti bolje razumijevanje širenja prekograničnih incidenata. Međunarodna suradnja među svim organizacijama koje sudjeluju u vježbi njen je sastavni dio i u njoj sudjeluje većina europskih zemalja. Vježba pruža iskustvo fleksibilnog učenja: sudionici mogu prilagoditi vježbu svojim potrebama odlučujući hoće li u njoj sudjelovati samo jedan analitičar ili cijela organizacija te u kojim će scenarijima sudjelovati, a u kojima ne. Kao i u prethodnoj vježbi koja se održala 2016. godine, u scenarij je ponovno bila uključena simulacija medijske pokrivenosti koja je, između ostalog, uključivala korištenje društvenih mreža, internetskog sjedišta poduzeća te raznih sigurnosnih blogova stoga ni ne iznenađuje kako je riječ o najrazvijenijoj vježbi u području kibernetičke sigurnosti u EU.

2.3. Vježba Cyber Coalition 2018

Hrvatska akademska i istraživačka mreža - CARNET i njezin odjel za Nacionalni CERT aktivno su sudjelovali u jedanaestoj po redu NATO vježbi zaštite NATO i nacionalnih računalnih sustava pod nazivom „Cyber Coalition 2018". U petodnevnoj vježbi koja je trajala od 26. do 30. studenog 2018. godine sudjelovalo je preko 700 sudionika iz 28 članica NATO-a , 4 partnerske zemlje NATO-a te tijela NATO-a i EU-a.

Vježba, između ostalog, obuhvaća obranu od zlonamjernog sadržaja (eng. *malware*) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti – *Cooperative Cyber Defence Centre of Excellence* (CCD COE) – koji se nalazi u Tallinnu u Estoniji.

2.4. ITU Cyber Drill – ALERT

Nacionalni CERT sudjelovao je u vježbi ITU Cyber Drill – ALERT (Applied Learning for Emergency Response Teams) for Europe Region koju je organizirao ITU (International Telecommunication Union) kroz inicijativu ciparskog CSIRT-a (National CSIRT-CY). Ovim petodnevnim događajem željelo se poboljšati komunikaciju i odgovor na incidente između timova koji su sudjelovali kao i osigurati daljnju suradnju CSIRT-ova u sprječavanju kibernetičkih prijetnji u regiji. Kroz cjelokupni događaj sudionici su imali priliku učiti o obradi računalno-sigurnosnih incidenata kroz trening koji je održala organizacija FIRST, razmijeniti iskustva na konferenciji o kibernetičkoj sigurnosti te vježbati spremnost na odgovore na računalno-sigurnosne incidente kroz dvodnevnu vježbu. Nacionalni CERT vježbu je prolazio u timu s rumunjskim CERT-om (CERT-RO) s kojim surađuje i kroz druge projekte i aktivnosti.

2.5. CSIRT mreža

Mreža CSIRT-ova 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 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 te 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 te razmjene informacija među CSIRT-ovima Europske Unije, poboljšanje operativnih procedura, podizanje razine zrelosti pojedinog CSIRT-a, odnosno razmjena 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.

2.6. MeliCERTes Stakeholder Expert Group

Nacionalni CERT nastavlja sudjelovanje u radu radne skupine MeliCERTes koja je oformljena za razvoj platforme za razmjenu informacija u Mreži CSIRT-ova. Platforma za razmjenu informacija o računalno-sigurnosnim incidentima razvija se u sklopu trogodišnjeg CEF projekta SMART 2015/1089. Platforma će objedinjavati skupine alata slobodnog softvera koje većinom koriste europski CSIRT-ovi kako bi se postigla brža razmjena informacija o računalnim prijetnjama i računalno-sigurnosnim incidentima. Tijekom 2018. predstavnici Nacionalnog CERT-a sudjelovali su na sastancima radne skupine na kojima se diskutiralo o trenutnim i budućim potrebama u radu MeliCERTes platforme kroz tri aspekta: tehnički, pravni te po pitanju potrebne podrške. Uz to smo sudjelovali u demonstracijama i testiranju do sada razvijenih funkcionalnosti te bili uključeni u pregleda napisanog kôda. U 2019. godini Nacionalni CERT će instalirati MeliCERTes platformu na vlastitoj infrastrukturi te se tako povezati sa zajednicom CSIRT-ova i unaprijediti razmjenu informacija na EU razini. Međunarodna suradnja među svim organizacijama koje sudjeluju u vježbi njen je sastavni dio i u njoj sudjeluje većina europskih zemalja. Vježba pruža iskustvo fleksibilnog učenja: sudionici mogu prilagoditi vježbu svojim potrebama odlučujući hoće li u njoj sudjelovati samo jedan analitičar ili cijela organizacija te u kojim će scenarijima sudjelovati, a u kojima ne. Kao i u prethodnoj vježbi koja se održala 2016. godine, u scenarij je ponovno bila uključena simulacija medijske pokrivenosti koja je, između ostalog, uključivala korištenje društvenih mreža, web sjedišta poduzeća te raznih sigurnosnih blogova stoga ni ne iznenađuje kako je riječ o najrazvijenijoj vježbi u području kibernetičke sigurnosti u EU.

2.7. DSI Governance Board

Nacionalni CERT aktivno sudjeluje u DSI programu (Cybersecurity Digital Service Infrastructures) koji je uspostavljen unutar CEF fondova (Connecting Europe Facility). Cilj CEF Cybersecurity DSI Governance Board programa je pružanje podrške CSIRT-ovima zemalja članica Europske unije u povećanju njihovih kapaciteta i suradnji s drugim timovima kroz mehanizme za razmjenu informacija. Mehanizmi za suradnju na operativnoj razini razvijaju se u projektu SMART 2015/1089, a CSIRT-ovi bi ih koristili na dobrovoljnoj bazi kako bi podržali zadatak povjeren CSIRT Network mreži prema NIS direktivi. Predstavnici Nacionalnog CERT-a sudjelovali su na radnim sastancima gdje su i prezentirali stanje i napredak u provođenju GrowCERT projekta.

3 Suradnja i djelovanje Nacionalnog CERT-a na nacionalnoj razini

3.1. Sporazum o poslovnoj suradnji s MUP-om

U 2018. godini nastavlja se suradnja na prevenciji i rješavanju računalno-sigurnosnih incidenata i drugih oblika računalnog kriminaliteta između MUP-a i CARNET-a (Nacionalnog CERT-a). Sporazumom koji je obnovljen krajem 2017. godine nastavlja se suradnja s ciljem očuvanja sigurnosti kibernetičkog prostora Republike Hrvatske. S obzirom na činjenicu da suvremeni način borbe protiv računalnog 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.

3.2. Sporazum o poslovnoj suradnji s FER-om

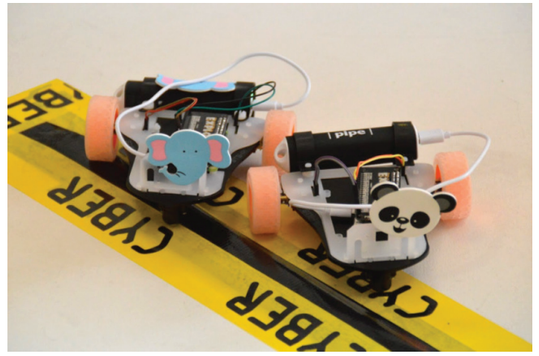
CARNET, odnosno njegov Odjel za Nacionalni CERT, nastavlja poslovnu suradnju s Fakultetom elektrotehnike i računarstva Sveučilišta u Zagrebu, odnosno Laboratorijem za sustave i signale Zavoda za elektroničke sustave i obradu informacija FER-a. Temeljem sporazuma potpisanog godinu prije, u 2018. godini objavljeno je 10 dokumenata, 10 recenzija alata i 38 novosti o zlonamjernom ransomware sadržaju koje je Laboratorij za sustave i signale (LSS) dostavio Nacionalnom CERT-u. Materijali se objavljuju na web sjedištima www.cert.hr i www.antibot.hr, a namijenjeni su obrazovanju i širenju znanja zainteresirane javnosti iz područja kibernetičke sigurnosti. U okviru poslova vezanih za provjeru sigurnosti računalnih programa, LSS na zahtjev CARNET-a izvršava provjeru sigurnosti računalne aplikacije. Osim toga, Nacionalni CERT dao je podršku Fakultetu elektrotehnike i računarstva u prijavi na projekt Horizon2020 (Letter of Intent) i time dao podršku kasnijim rezultatima projekta, posebice naporima za podizanje svijesti i obrazovanje stručnjaka u području kibernetičke sigurnosti i cjelokupne javnosti.

3.3. Vježba Kibernetički štit 2018

U organizaciji Samostalnog sektora za informacijske i komunikacijske sustave MORH-a te Glavne planske skupine 15. ožujka 2018. godine održana je prva vježba Koordinacije za sustav domovinske sigurnosti pod nazivom „Kibernetički štit 2018". Vježba je okupila članove Koordinacije na čelu s potpredsjednikom Vlade i ministrom obrane Damirom Krstičevićem, a u ulozi promatrača nazočili su i predstavnici drugih institucija. Kibernetički štit 2018 je simulacijska vježba temeljena na scenariju kibernetičkog napada u kojoj su ključni donositelji odluka na nacionalnoj razini okupljeni u Koordinaciji za sustav domovinske sigurnosti imali mogućnost provjeriti funkcioniranje sustava upravljanja u kriznim situacijama. CARNET je u vježbi sudjelovao u ulozi promatrača.

3.4. FSec IoT Hacking Summer School

Nekoliko djelatnika CARNET-a sudjelovalo je u ljetnoj školi "FSec IoT Hacking Summer School" u organizaciji Fakulteta organizacije i informatike u Varaždinu. U tjedan dana imali su priliku učiti od domaćih i stranih stručnjaka iz područja kibernetičke sigurnosti. Pričalo se o aktualnim i zanimljivim temama kao što su hakiranje autonomnih vozila, SCADA sustavima, steganografiji, mrežnoj forenzici itd., a svi sudionici imali su priliku sudjelovati u CTF natjecanju (eng. *Capture the flag*). Važno je napomenuti i kako je CARNET pružio tehničku podršku, odnosno zaposlenik u CARNET-ovom odjelu multimedije snimao je sva predavanja i CTF te time pridonio kvaliteti ljetne škole.



Dron zaposlenika CERT-a na CTF natjecanju (desno)

3.5. Vodič ICC-a za informacijsku sigurnost u poslovanju

Hrvatska gospodarska komora i Međunarodna trgovačka komora Hrvatska (ICC Hrvatska) u suradnji s nacionalnim partnerima, među kojima je i CARNET, predstavila je u ožujku Vodič ICC-a za informacijsku sigurnost u poslovanju. Na panel raspravi sudjelovao je pomoćnik ravnatelja za Nacionalni CERT, a tema panela bila je „Izazovi informacijske sigurnosti iz prakse poslovanja hrvatskih poduzeća". Vodič na pristupačan način pojašnjava osnove informacijske sigurnosti u poslovanju, upozorava na sigurnosne ugroze i rizike poslovanja na internetu te nudi praktična rješenja za učinkovitije upravljanje rizikom. Navodi načela i postupke koji će pomoći u postizanju

bolje informacijske sigurnosti, a sadrži i upitnik za samoprocjenu stanja informacijske sigurnosti u poduzeću. Vodič je namijenjen poduzećima svih veličina i iz svih sektora gospodarstva, vlasnicima poduzeća, menadžmentu i zaposlenicima te nije ograničen samo na IT službe.

3.6. (O)siguran online

Nacionalni CERT je uz stručnjake iz Društva za komunikacijsku i medijsku kulturu sudjelovao u projektu Wiener Osiguranja "(O)siguran online" u sklopu kojega su izrađeni materijali kojima se roditelje savjetuje o sigurnosti djece u online svijetu. Izrađen je online upitnik za roditelje, ilustrirani vodič za roditelje i djecu te edukativni video materijali u kojima su situacije iz života poznatih osoba iz Hrvatske komentirali relevantni stručnjaci. Projekt je nagrađen nagradom za korporativnu sigurnost Hrvatske udruge menadžera sigurnosti u kategoriji „Društvena odgovornost na području zajednice". Samim projektom je na društvenoj mreži Facebook dosegnuto 352.988 ljudi, dok su oglasi prikazani ukupno 1.663.850 puta.

3.7. Nacionalna strategija kibernetičke sigurnosti (NSKS)

U 2018. godini Nacionalni CERT nastavio je rad na provedbi mjera iz Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti (NSKS). Kako je riječ o prvoj sveobuhvatnoj Strategiji u RH na području kibernetičke sigurnosti, primarni je cilj Strategije prepoznavanje organizacijskih problema u njezinoj provedbi te širenje razumijevanja važnosti ove problematike u društvu. Poticanje koordinacije i suradnje svih državnih tijela i pravnih osoba s javnim ovlastima, ali i drugih sektora društva, nužno je kako bi se uspostavile nove funkcionalnosti, podigla učinkovitost rada relevantnih sudionika te učinkovitije koristilo postojeće resurse i bolje planiralo potrebu i ostvarenje novih resursa. Nacionalni CERT aktivno sudjeluje u radu Nacionalnog vijeća za kibernetičku sigurnost (NVKS) i Operativno-tehničke koordinacije za kibernetičku sigurnost (OTKKS), tijelima osnovanim odlukom Vlade polovicom 2016. godine s ciljem provedbe Nacionalne strategije kibernetičke sigurnosti i Akcijskog plana za provedbu Strategije. Sjednice NVKS-a i OTKKS-a održavaju se jednom mjesečno, osim u iznimnim slučajevima ako postoji potreba za sazivanjem izvanrednih sjednica. U 2018. godini sjednice su se održavale redovito (12 sjednica NVKS-a od ukupno 23 i 12 sjednica OTKKS-a od ukupno 22).

Mjere u kojima Nacionalni CERT aktivno sudjeluje su:

- razvoj međusektorske suradnje nacionalnih regulatornih tijela i tijela odgovornih za područje kibernetičke sigurnosti i politike zaštite podataka te međusobna koordinacija i razmjena iskustava u suradnji i zahtjevima koji proizlaze iz međunarodnih okvira;
- definiranje taksonomije (uključujući pojam značajnog incidenta), definiranje protokola za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima te uspostava platforme ili tehnologije za razmjenu podataka;
- razmjena prethodno anonimiziranih podataka o incidentima između sektorski nadležnih tijela korištenjem definirane taksonomije i protokola;
- izvještavanje dionika unutar sektora o računalno-sigurnosnim incidentima te periodično izvještavanje Nacionalnog vijeća za kibernetičku sigurnost o trendovima, stanju i značajnim incidentima iz prethodnog razdoblja;
- izdavanje upozorenja o sigurnosnim ugrozama i trendovima te odgovarajućih preporuka za postupanje;
- izobrazba zaposlenika na godišnjoj razini za potrebe ekspertize i specijalističke izobrazbe;
- izrada i objavljivanje preporuka o minimalnim sigurnosnim zahtjevima za davatelje i korisnike različitih elektroničkih usluga, kao i javno i komercijalno dostupnih bežičnih mreža (Wi-Fi) koje postaju masovno korištene, s ciljem zaštite krajnjih korisnika takvih usluga koji su široko zastupljeni u svim sektorima društva;
- osmišljavanje i provođenje usklađene kampanje o podizanju svijesti svih korisnika, odnosno vlasnika javno dostupnih sustava u Republici Hrvatskoj, o značaju kibernetičke sigurnosti.

3.8. NIS direktiva

Kroz rad stručne radne skupine Nacionalnog vijeća za kibernetičku sigurnost za provedbu obveza Republike Hrvatske u području NIS direktive Europske unije, Nacionalni CERT sudjelovao je u pripremi prijedloga Zakona i Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga koji su doneseni u srpnju 2018. godine. Donošenje takvog Zakona proizlazi iz obveza Hrvatske kao članice EU-a za prijenos NIS direktive u nacionalno zakonodavstvo. NIS direktiva, punog naziva Direktiva o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, donesena je 6. srpnja 2016. temeljem provedbe Europske strategije kibernetičke sigurnosti iz 2013. godine, a s ciljem osiguravanja zajedničke razine sigurnosti mrežnih i informacijskih sustava u svim državama članicama. NIS direktiva utvrđuje obvezu država članica o uvođenju mjera za visoku razinu zaštite kibernetičke sigurnosti u ključnim sektorima. U skladu s navedenim Zakonom i Uredbom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga, operatori ključnih usluga i davatelji digitalnih usluga dužni su, bez neopravdane odgode, obavještavati nadležni CSIRT o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju. 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. Nadležni CSIRT-ovi (CERT Zavoda za sigurnost informacijskih sustava i Nacionalni CERT) donijeli su Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga. Uz to, izrađeni su obrasci "Inicijalna obavijest", "Prijelazno izvješće" i "Završno izvješće" prema kojima su operatori ključnih usluga i davatelji digitalnih usluga dužni prijavljivati incidente sa znatnim učinkom nadležnom CSIRT-u. Modul "Prijava incidenta prema ZKS-u" može se pronaći na web sjedištu www.cert.hr.

3.9. Djelovanje putem javnih medija i obraćanja javnosti

S ciljem podizanja svijesti o kibernetičkoj sigurnosti Nacionalni CERT djelovao je kroz sljedeće aktivnosti:

- 1/2018 – izmijenjen vizualni identitet CARNET-a, Nacionalni CERT dobiva novi logo i koristi ime CERT.hr;
- 1/2018 – predavanje „Socijalni inženjering – Čovjek kao najveća ranjivost sustava“ na Županijskom stručnom vijeću;
- 2/2018 – webinar „Wanna Cry – Dani nesigurnog interneta“ povodom obilježavanja Dana sigurnijeg interneta;
- 2/2018 – Sudjelovanje na okruglom stolu na temu „Cyber prijetnje u korporativnom sektoru“;
- 2/2018 – Izmijenjen izgled web sjedišta cert.hr na kojem su dodane i nove kategorije;
- 3/2018 – Dnevnik Nove TV – prilog o curenju podataka na društvenoj mreži Facebook i „Cambridge Analytica“ skandalu;
- 3/2018 – Otvorena Facebook stranica CERT.hr
- 4/2018 – HRT emisija „Potrošački kod“ – prilog o curenju podataka na društvenoj mreži Facebook i „Cambridge Analytica“ skandalu;
- 5/2018 – emisija „RTL Direkt“ – prilog o zaštiti osobnih podataka;
- 6/2018 – objavljena „Nacionalna taksonomija računalno-sigurnosnih incidenata“;
- 10/2018 – U suradnji s agencijama ENISA i APWG objavljena „phishing“ infografika i time je obilježen početak Mjeseca kibernetičke sigurnosti koji se svake godine na međunarodnoj razini obilježava u listopadu (eng. *Cyber Security Month*)
- 10/2018 – Održano predavanje u Centru za mlade Samobor (Bunker) na temu sigurnosti djece na internetu
- 10/2018 – Vijesti Radija 101 – upozorenje o ucjenjivačkim „scam“ mailovima
- 10/2018 – Održano predavanje u Erste banci u sklopu godišnjeg sastanka korporativne sigurnosti
- 10/2018 – Sudjelovanje na četvrtom po redu hrvatskom Forumu o upravljanju internetom (CRO-IGF) u panelu „Otpornost demokracije na kibernetičke napade“
- 10/2018 - Održan okrugli stol „Ususret europskoj godini kibernetičke sigurnosti“ u organizaciji Hrvatske akademske i istraživačke mreže – CARNET, a u sklopu Europskog mjeseca kibernetičke sigurnosti
- 11/2018 - Sudjelovanje na CARNET-ovoj korisničkoj konferenciji „CUC2018“ s temama „#SurfajSigurnije“, „Dani nesigurnog interneta – ransomware“ i „Sigurnost kao proces“
- 11/2018 - Sudjelovanje na Konferenciji o sigurnosti informacijskih sustava 2018. s prezentacijom “Kibernetička sigurnost: čovjek u centru sigurnosnih procesa”
- informiranje javnosti putem web sjedišta Nacionalnog CERT-a (www.cert.hr) – 319 634 posjetitelja u 2018. godini
- Informiranje javnosti putem društvenih mreža Facebook (@CERT.hr - 995 pratitelja) i Twitter (@HRCERT – 763 pratitelja)

4 Projekti

4.1. GrowCERT

Nacionalni CERT i CARNET, potaknuti stvaranjem doprinosa ostvarivanju ciljeva Nacionalne strategije kibernetičke sigurnosti, pokrenuli su 1. srpnja 2017. godine dvogodišnji projekt pod nazivom GrowCERT – Jačanje kapaciteta Nacionalnog CERT-a i poboljšanje suradnje na nacionalnoj i europskoj razini. Projekt u vrijednosti od gotovo 985 000 eura sufinanciran je sredstvima Europske komisije putem Instrumenta za povezivanje Europe (CEF – Connecting Europe Facility). Provedbom projekta doprinosi se jačanju nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti korištenjem novorazvijene platforme za prikupljanje podataka o sigurnosnim incidentima na nacionalnoj i europskoj razini. Ovim projektom želi se podići svijest o kibernetičkim prijetnjama te adekvatnim odgovorima na iste. Prema kreativnom konceptu nacionalne kampanje podizanja svijesti o kibernetičkoj sigurnosti provedena je javna nabava za produkciju kampanje kojom će se u prvom kvartalu 2019. godine provoditi niz marketinških i medijskih aktivnosti kojima se želi podići svijest o kibernetičkoj sigurnosti opće populacije, a posebno poslovnog sektora i akademske zajednice. Projektom je omogućeno dodatno ulaganje u ljudske i tehničke kapacitete Nacionalnog CERT-a. Tijekom 2018. godine Nacionalni CERT je razvio nove usluge: DNSBL sustav za blokiranje neželjene pošte (eng. *spam*), CVE search - sustav za distribuciju informacija o otkrivenim ranjivostima i alat za otkrivanje izmijenjenih izgleda stranica web sjedišta (eng. *web defacement*) te drugih zlonamjernih sadržaja u kibernetičkom prostoru u ovlasti Nacionalnog CERT-a. Uz savjetodavnu pomoć tvrtke Ernst & Young Savjetovanje d.o.o. započeo je razvoj i uspostava platforme za prikupljanje, analizu i razmjenu podataka o sigurnosnim incidentima. U tom procesu sudjeluje stručna radna skupina sastavljena od predstavnika različitih sektora (MORH, MUP, HANFA, HNB, HAKOM, Hrvatska udruga banaka, Zavod za sigurnost informacijskih sustava i akademska zajednica) koja je sudjelovala u definiranju sadržaja Nacionalne taksonomije računalno-sigurnosnih incidenata, izradi konceptualnog dizajna platforme i njene funkcionalne specifikacije. U nastavku projekta slijede korisnička i sigurnosna testiranja platforme. Projekt je predstavljen nacionalnoj, europskoj i međunarodnoj sigurnosnoj zajednici na brojnim konferencijama i sastancima.

grow-cert

4.2. Grow2CERT

Nacionalni CERT je u studenom prijavio novi projekt za sufinanciranje iz Instrumenta za povezivanje Europe (CEF – Connecting Europe Facility) pod nazivom Grow2CERT, a s ciljem povećanja zrelosti Nacionalnog CERT-a za snažniju suradnju u kibernetičko-sigurnosnoj zajednici (eng. *Increasing maturity of National CERT for stronger cooperation in cybersecurity community*). Nacionalni CERT u sklopu projekta GrowCERT radi na integraciji i pripremi komponenata Nacionalne platforme za interakciju s MeliCERTes-om (platforma za razmjenu informacija o kibernetičko-sigurnosnim incidentima u Mreži CSIRT-ova). Cilj predloženog projekta je povećati spremnost Nacionalnog CERT-a i integrirati dodatne komponente Nacionalne platforme koje će omogućiti interakciju s MeliCERTes i njihovo korištenje. Stvaranje novih komponenti na postojećoj Nacionalnoj platformi, kao i poboljšanje kapaciteta Nacionalnog CERT-a i drugih nacionalnih tijela koja sudjeluju u provedbi računalno-sigurnosnih mjera, nabava opreme i licenci povećat će nacionalne računalno-sigurnosne kapacitete i omogućiti interakciju s MeliCERTes-om na više razina. Cilj je također poboljšati Nacionalnu platformu u skladu s NIS Direktivom, posebno uključujući operatore ključnih usluga i davatelje digitalnih usluga u prikupljanje i razmjenu informacija o incidentima i prijetnjama putem Nacionalne platforme. Opseg projekta čini osam različitih aktivnosti. Uz upravljanje projektom i komunikaciju i vidljivost, ostale aktivnosti odnose se na nadogradnju nacionalne platforme i pripremu za korištenje komponenti MeliCERTes-a, aktivnosti podizanja svijesti, povećanje razine zrelosti Nacionalnog CERT-a na temelju SIM3 kriterija, poboljšanje kapaciteta osoblja CERT-a i drugih nacionalnih tijela koja sudjeluju u provedbi mjera kibernetičke sigurnosti, organizacija sastanka Mreže CSIRT-ova u sklopu predsjedanja te nabava opreme i licenci za podizanje ukupne razine kibernetičke sigurnosti.

4.3. e-Škole: Uspostava sustava razvoja digitalno zrelih škola (pilot projekt)

U sklopu projekta "e-Škole: Uspostava razvoja digitalno zrelih škola (pilot projekt)" Nacionalni CERT je poduzimanjem niza proaktivnih mjera spriječio eventualne ugroze sigurnosti usluga razvijenih za potrebe projekta. Nabavkom opreme i softvera potrebnih za provođenje sigurnosnih testiranja te edukacijom zaposlenika na području informacijske sigurnosti značajno su poboljšani kapaciteti Nacionalnog CERT-a. Stručnjaci Nacionalnog CERT-a su u suradnji s izvođačima proveli nekoliko iteracija sigurnosnih testiranja za šest ključnih usluga koje će pomoći školama u informatizaciji nastavnih i nenastavnih procesa te povećati opću kvalitetu i poslovanje škole. Rezultat sigurnosnih testiranja povećanje je razine sigurnosti cijelog ekosustava e-Škole usluga. Projekt je završio 31. kolovoza 2018. godine.

e-Škole

4.4. GEANT4

Nacionalni CERT sudjelovao je u četvrtoj generaciji projekta GEANT – GEANT4.2. Projekt je sufinanciran sredstvima Europske unije, a glavni cilj je razvoj paneuropske akademske i istraživačke e-infrastrukture koja je prepoznata kao temelj za poticanje znanstvene izvrsnosti i interoperabilnosti. Nacionalni CERT sudjelovao je u aktivnostima vezanim uz uspostavu okvira za implementaciju sigurnosti u GEANT-ovoj infrastrukturi i uslugama, izradi okvira za sustavni razvoj, održavanje i unaprjeđivanje GEANT-ovih usluga (eng. *Software Management Framework*) te na poslovima sigurnosnih testiranja GEANT-ovih usluga. Projektne aktivnosti provodile su se u sklopu servisne aktivnosti (eng. *Service Activity*) SA2. Uspostavljeni su mehanizmi kvalitativne i sigurnosne provjere novih usluga tijekom tranzicije usluga iz razvojnog okruženja u produkciju te periodičkih provjera produkcijskih usluga. U skladu s uspostavljenim okvirom obavljene su kvalitativne i sigurnosne provjere pet novih GEANT-ovih usluga koje su tijekom godine uspješno uključene u produkcijsko okruženje. Osim sigurnosnih provjera Nacionalni CERT je sudjelovao u izradi javnog dokumenta "Service Transitions and Validations" kojim je opisan proces tranzicije GEANT-ovih usluga u produkcijsko okruženje. Projekt je završio 31. prosinca 2018. godine.

GÉANT

4.5. Cyber Exchange

U studenom 2018. godine započeo je projekt „CyberExchange" u okviru Instrumenta za povezivanje Europe – Connecting Europe Facility (CEF). Nositelj projekta je udruženje CZ.NIC iz Češke, a u projektu sudjeluje 10 država Europske unije (Austrija, Hrvatska, Češka, Grčka, Latvija, Luksemburg, Malta, Poljska, Rumunjska i Slovačka). Projekt će trajati dvije godine, a cilj mu je jačanje suradnje između nacionalnih i državnih CSIRT-ova/CERT-ova. CyberExchange je pokrenut radi poboljšanja odaziva na sve učestalije prijetnje kibernetičkoj sigurnosti te naglašava važnost prekogranične suradnje u njihovom suzbijanju. Osim toga, važna je i stručnost osoba koje rade u području kibernetičke sigurnosti. Tijekom projekta održat će se razmjena djelatnika CERT-ova/CSIRT-ova tijekom koje će individualni članovi pojedinih timova imati priliku razmijeniti iskustva te unaprijediti svoju stručnost. Projektom se također stavlja fokus na implementaciju softverskih alata koje su razvili timovi uključeni u projekt kako bi se koristili na dobrobit cijele sigurnosne zajednice. Projekt podržava i MeliCERTes platformu te Centre za sigurniji internet.

Cyber Exchange

5 Stanje računalnih incidenata i statistike

5.1. Nacionalna taksonomija računalno-sigurnosnih incidenata

U 2018. godini izrađena je "Nacionalna taksonomija računalno-sigurnosnih incidenata" nastala temeljem Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti, a u okviru provedbe projekta GrowCERT. Taksonomija je rezultat suradnje Zavoda za sigurnost informacijskih sustava (ZSIS) i Nacionalnog CERT-a, a pri realizaciji podršku je pružila radna skupina sastavljena od predstavnika tijela različitih sektora, HAKOM-a, HNB-a, MORH-a, MUP-a, HANFA-e te stručnjaka s FER-a i FOI-a.

Akcijski plan kao cilj G.1 navodi "kontinuirano unaprjeđivati postojeće sustave za prikupljanje, analizu i pohranu podataka o računalno-sigurnosnim incidentima te voditi brigu o ažurnosti drugih podataka bitnih za brzu i efikasnu obradu takvih incidenata", a mjerom G.1.1 nastoji se "definirati taksonomije, uključujući pojam značajnog incidenta, definirati protokole za razmjenu anonimiziranih podataka o značajnim sigurnosnim incidentima, te uspostaviti platformu ili tehnologiju za razmjenu podataka".

"Nacionalna taksonomija računalno-sigurnosnih incidenata" važna je jer daje definiciju pojma računalno-sigurnosnog incidenta te nudi ujednačene kriterije pri klasifikaciji računalno-sigurnosnih incidenata na nacionalnoj razini u svojim informacijskim sustavima i računalnim mrežama, a njome se žele stvoriti preduvjeti da sva tijela i institucije koje će razmjenjivati informacije o računalno-sigurnosnim događajima to čine tako da su svim sudionicima u toj razmjeni u potpunosti jasni i kontekst i detalji o pojedinom događaju ili incidentu.

Izradom "Nacionalne taksonomije računalno-sigurnosnih incidenata" pokriven je dio mjere G.1.1 Akcijskog plana za provedbu Nacionalne strategije kibernetičke sigurnosti te je ostvaren jedan od rezultata projekta GrowCERT.

Kod obrade incidenata Nacionalna taksonomija počela se primjenjivati od 1. kolovoza 2018. godine. Statistika u nastavku koja se odnosi na incidente po tipu ujedinjena je za cijelu 2018. godinu i iz tog razloga se ne podudara u potpunosti s novom taksonomijom. Važno je napomenuti i kako je navedena taksonomija „živi" dokument koji će se, u suradnji sa ZSIS-om i radnom skupinom, mijenjati ovisno o potrebama.

5.2. Statistika o obrađenim incidentima

Nacionalni CERT je tijekom 2018. godine zaprimio i obradio ukupno 684 prijave koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a.

Vodeći tipovi incidenata su ***web defacement*** (kompromitirano web sjedište s izmijenjenim izgledom ili sadržajem web stranice), ***phishing URL*** i ***hoax***.

Najznačajnija promjena u odnosu na prošlu godinu je velik broj *hoax* incidenata. Radi se o ucjenjivačkim „scam" porukama koje je velik broj korisnika zaprimilo na svoje adrese elektroničke pošte. Napadači pokušavaju iznuditi novčanu dobit od žrtve navodeći da će objaviti navodne osjetljive podatke od žrtve ako se ne izvrši uplata u Bitcoin vrijednosti. Kako je *hoax* kao tip incidenta definiran tek novom taksonomijom, broj od 65 takvih incidenata odnosi se na incidente koji su se prijavljivali od 1. kolovoza do 31. prosinca 2018. godine. Bez obzira na to, *hoax* je uspio doći na treće mjesto incidenata po tipu u 2018. godini.

Velika promjena odnosi se i na pad broja web *defacement* incidenata kojih je u 2018. godini bilo 102 manje nego u 2017. godini. Veliki pad nije utjecao na pomicanje web *defacement* incidenata prema broju, te se i dalje nalazi na prvom mjestu obrađenih incidenata prema tipu.

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 u odnosu na prethodnu godinu smanjio se za 26%.

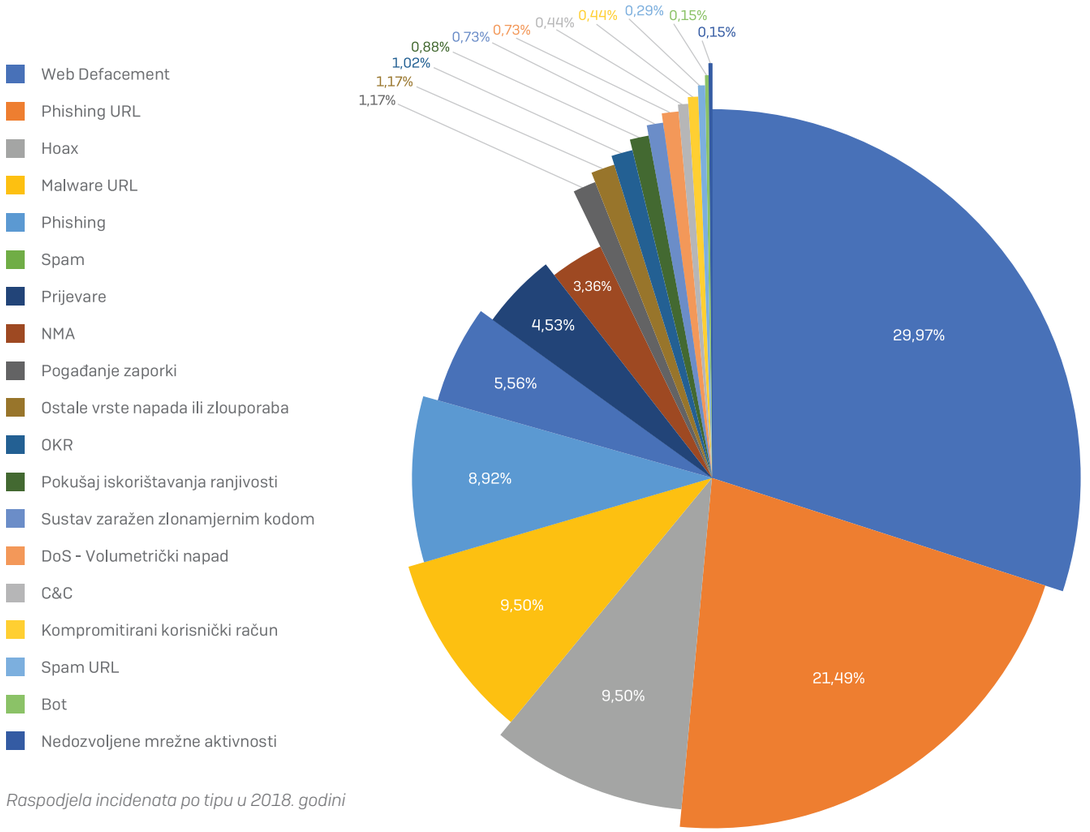
TIP INCIDENTA	BROJ	TREND
Web defacement	205	▼
Phishing URL	147	▲
Hoax	65	–
Malware URL	65	▲
Phishing	61	▲
Spam	38	▲
Prijevare	31	–
NMA	23	▼
Pogađanje zaporki	8	–
Ostale vrste napada ili zlouporaba	8	▼
OKR	7	▲
Pokušaj iskorištavanja ranjivosti	6	–
Sustav zaražen zlonamjernim kodom	5	–
DoS - Volumetrički napad	5	▼
C&C	3	▲
Kompromitirani korisnički račun	3	–
Spam URL	2	▼
Bot	1	▼
Nedozvoljene mrežne aktivnosti	1	▼
UKUPNO	684	▼

Prikaz incidenata po tipu u 2018. godini

5.3. Raspodjela incidenata po tipu

Sljedeći grafikoni prikazuju omjere incidenata po tipu u 2018. godini koji su zabilježeni u sustavu za obradu incidenata. Svi incidenti su ujedinjeni u grafikonu bez obzira na promjenu taksonomije.

Incidenti su se prijavljivali putem adrese elektroničke pošte incident@cert.hr ili su prijave dobivene od vanjskih izvora kroz automatizirane softvere za obradu incidenata.

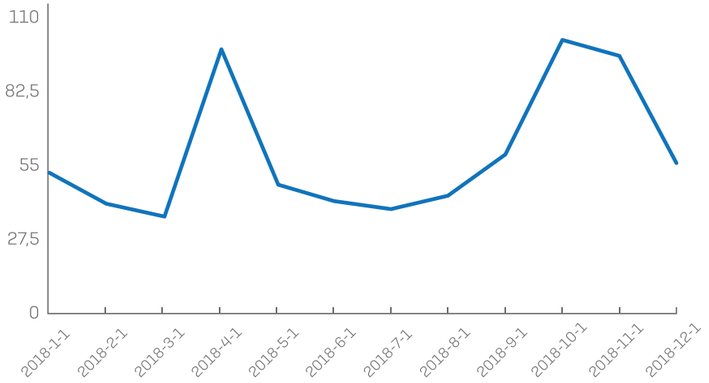


Raspodjela incidenata po tipu u 2018. godini

5.4. Trendovi pojava incidenata na poslužiteljima u 2018. godini

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

Najveći broj incidenata zabilježen je i obrađen u listopadu 2018. godine, njih 101. Najmanji broj incidenata zabilježen je u srpnju kada su obrađena 33 incidenta. Prosječan broj incidenata mjesečno iznosi 57 incidenata.



Broj incidenata koje je 2018. godine obradio Nacionalni CERT s prikazom po mjesecima

5.5. Registrirani *botovi* u Republici Hrvatskoj

Nacionalni CERT primao je i statistički obrađivao podatke o botovima na računalima krajnjih korisnika. Podaci su prosljeđivani pripadajućim davateljima internetskih usluga i pružateljima usluga udomljavanja internetskih stranica (eng. *hosting provider*). Iz grafikona koji prikazuje godišnji trend broja botova moguće je očitati da je u Hrvatskoj broj registriranih zaraženih računala u padu te da ih u odnosu na prethodnu godinu ima manje. Broj otkrivenih botova prikazan ovim statistikama temelji se na vanjskim izvorima koji dostavljaju podatke Nacionalnom CERT-u te ne odgovara broju stvarno zaraženih korisničkih računala, ali prikazuje trend i okvir stvarnog stanja.

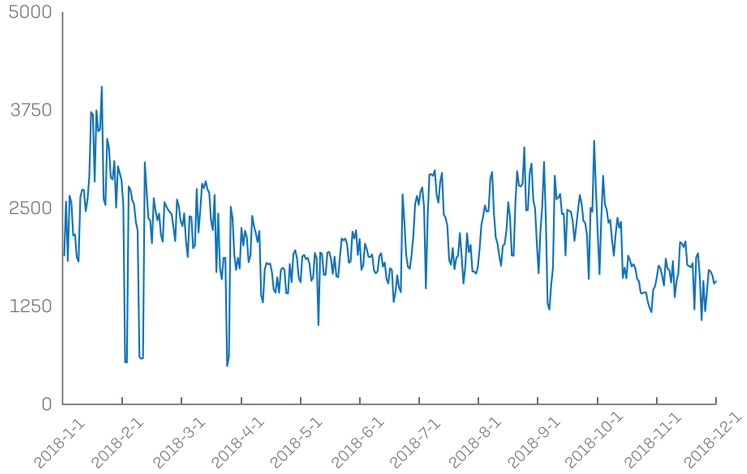
U tablici u nastavku prikazano je deset najčešće prijavljivanih botova prema tipu (vrsti zlonamjernog sadržaja) kroz 2017. godinu, koji su bili diseminirani davateljima usluge pristupa internetu.

Avalanche-andromeda	260 061
Conficker	136 891
Mirai	100 628
Unknown	47 453
gamarue	29 858
Gamut	26 953
Wannacrypt	17 211
Sality-p2p	17 141
Sality	14 606
Monerominer	8 620

Top 10 botova prema tipu u 2018. godini

Suma zabilježenih *botova* prema tipu (vrsti zlonamjernog sadržaja) tijekom 2018. godine iznosi 746 160, što je povećanje od visokih 85 % u odnosu na 2017. godinu. Veliko povećanje rezultat je dodavanja dva nova izvora iz kojih se podaci povlače u sustav.

Broj zabilježenih *botova* po danima u 2018. godini prikazan je u nastavku. Prema trendu kretanja poznatih *botova* u Hrvatskoj može se zaključiti da se uglavnom kreću iznad 2000 *botova* dnevno, što nije bio slučaj prošle godine.



Srednja vrijednost broja botova po danu za 2018. godinu iznosila je 2.052,82.

5.6. 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 2018. godine služba CARNET Abuse obradila je ukupno 1399 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.Najveći postotak 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 drugom slučaju, korisnike se redovito upućuje na portal antibot.hr kako bi skenirali računalo i očistili ga od zlonamjernog sadržaja.

6 Značajniji incidenti, otkrivene ranjivosti i događaji

1. kvartal

- Prvi dan 2018. godine obilježila je zero-day ranjivost macOS operacijskog sustava stara 15 godina. Ranjivost je lokalnom napadaču omogućavala stjecanje root ovlasti nad ciljanim uređajem te pokretanje proizvoljnog zlonamjernog programskog koda. Ranjivost je nazvana IOHIDeous, a pogađala je IOHIDFamily funkcionalnost, odnosno funkcionalnost jezgre operacijskog sustava macOS koja je vezana uz korisničko sučelje poput ekrana osjetljivog na dodir.
- Sredinom siječnja zabilježena je phishing kampanja prema korisnicima CARNET Webmail servisa. Poruka elektroničke pošte koju su korisnici dobivali na svoje adrese sadržavala je poveznicu na phishing stranicu. U rješavanje incidenta uključio se i CERT Zavoda za informacijsku sigurnost jer je u incident bilo uključeno i jedno tijelo iz njihove nadležnosti.
- Krajem siječnja na Dark Webu nudili su se osobni podaci američke novorođenčadi za 300 američkih dolara. Ovakvi podaci potencijalno se mogu iskoristiti za dizanje kredita, ugovaranje usluge kartičnog plaćanja i slično. Krađe identiteta djece mogu ostati neotkrivene godinama tj. sve do trenutka kada se osoba s tim identitetom ne odluči za iskorištavanje ranije spomenutih povlastica. Upravo iz tog razloga ovi su podaci veoma vrijedni te napadači koriste sve metode zaštite kako bi prikrili svoj stvarni identitet.
- Na kraju mjeseca siječnja prijavljena je kompromitacija AAI@EduHr korisničkog računa koji se koristio kao pristupni podatak za određene CARNET-ove usluge.
- Početkom veljače pojavio se sve veći broj slučajeva povezanih s ranjivostima Meltdown i Spectre. Sigurnosna tvrtka AV-TEST navodi kako je otkrila 139 sumnjivih datoteka koje su vezane uz prethodno spomenute ranjivosti. Posebno je zabrinjavajuća činjenica kako su se na stranici VirusTotal počele pojavljivati inačice zlonamjernog sadržaja koje koriste ove dvije ranjivosti.
- Swisscom, najveća telekom kompanija u Švicarskoj, početkom veljače je doživjela veliko neovlašteno otkrivanje podataka svojih korisnika. U ovom slučaju riječ je o oko 800 000 korisnika što je jednako 10% cjelokupne švicarske populacije. Podaci kojima je pristupljeno sastojali su se od imena i prezimena, kućne adrese, datuma rođenja te telefonskih brojeva korisnika Swisscoma. Podaci su karakterizirani kao "ne-osjetljivi" unutar švicarskog zakona o zaštiti podataka. Osjetljivi podaci poput lozinki i transakcijskih potvrda nisu izloženi riziku.
- Europol je krajem ožujka objavio kako je španjolska policija uhitila osobu za koju se vjeruje da stoji iza zloglasne hakerske skupine Carbanak koja je poznata po nekim od najvećih napada na banke u posljednjih nekoliko godina. Prema podacima što ih je objavio Europol, skupina Carbanak, također poznata kao skupina Cobalt, izvela je preko 100 napada u 40 različitih zemalja te ukrala više od milijardu eura što u prosjeku iznosi 10 milijuna eura po napadu.
- Na kraju prvog kvartala Nacionalni CERT je poslao sigurnosno upozorenje o izdanoj zakrpi za otklanjanje visoko kritične ranjivosti u jezgri Drupal CMS-a inačica 6.x (End of Life), 7.x i 8.x. Obavijest je prenesena svim CARNET sistem inženjerima na ustanovama članicama te većim hrvatskim pružateljima udomljavanja internet stranica.

2. kvartal

- Početkom travnja internetski servis Hashes.org dodao je mogućnost preuzimanja baze lozinki iz alata Pwned Passwords. Pwned Passwords dio je stranice Have I Been Pwned koja je pokrenuta 2013. godine kako bi pomogla žrtvama čiji su podaci kompromitirani. Nakon objave nove inačice alata, u bazi se nalazi 501 milijun lozinki. Hashes.org omogućuje korisnicima provjeru je li im lozinka kompromitirana bez da koriste online servis Pwned Passwords.
- Sredinom travnja u hrvatskom IP adresnom prostoru detektiran je C&C upravljački poslužitelj za Loki botnet. Iz baze su izvučene IP adrese s kojima je C&C komunicirao. Pripadajućim stranim ISP-evima i CERT-ovima poslan je popis IP adresa kako bi upozorili vlasnike kompromitiranih korisničkih računala.
- Početkom svibnja otkrivena je nova metoda napada putem mrežnih paketa nazvana „Throwhammer". Sigurnosni stručnjaci sa Sveučilišta Vrije u Amsterdamu te Sveučilišta na Cipru otkrili su način kako pokrenuti Rowhammer napad putem mrežnih paketa i mrežnih kartica (metodu su nazvali „Throwhammer"). Njihovo otkriće čini izvođenje Rowhammer napada mnogo jednostavnijim od prethodnih metoda koje su od napadača zahtijevale da zarazi žrtvu zlonamjernim sadržajem ili da je navedu na internetsku stranicu sa zlonamjernim sadržajem putem koje bi žrtve preuzimale Rowhammer na računalo putem JavaScripta.
- Sredinom svibnja grupa europskih istraživača za računalnu sigurnost izdala je upozorenje o nekoliko ranjivosti koje zahvaćaju korisnike PGP i S/MIME alata. Electronic Frontier Foundation (EFF) u suradnji s navedenim istraživačima potvrđuje da ove ranjivosti dovode u rizik korisnike koji navedene alate koriste za komunikaciju elektroničkom poštom, a izložene mogu biti i prethodno šifrirane poruke.
- 25. svibnja na snagu je stupila Opća uredba o zaštiti osobnih podataka (GDPR – General Data Protection Regulation). Zaštita osobnih podataka jedan je od osnovnih zadataka koje GDPR stavlja pred organizacije bilo da je riječ o osobnim podacima korisnika, klijenata ili zaposlenika. Organizacije u svakom trenutku moraju znati gdje su koji podaci te u koju svrhu se smiju koristiti.
- Početkom lipnja zaprimljen je podatak o C&C upravljačkom poslužitelju za Loki botnet (nije isti slučaj kao iz travnja). Pripadajućim stranim ISP-evima i CERT-ovima poslan je popis IP adresa kako bi upozorili vlasnike kompromitiranih korisničkih računala.
- Sredinom lipnja prijavljeno je nekoliko slučajeva od ranije poznate tzv. „CEO fraud" phishing poruke u kojoj se pošiljatelj lažno predstavlja u ime visokopozicionirane osobe na ciljanoj ustanovi/instituciji s namjerom stjecanja novčanih sredstava.
- Krajem lipnja proizvođač sportske odjeće Adidas objavio je kako je došlo do curenja podataka o korisnicima koji su koristili njihovu američku stranicu. Prema rezultatima tada aktivne istrage, može se zaključiti da su podaci sadržavali osobne informacije, korisnička imena i lozinke, no podaci bankovnih kartica korisnika nisu objavljeni.

3. kvartal

- Početkom srpnja Facebook je priznao kako je omogućio nizu razvojnih programera te tehnoloških tvrtki pristup do korisničkih podataka nakon što su 2015. godine objavili da su onemogućili vanjskim tvrtkama pristup do podataka. Tijekom skandala vezanog uz tvrtku Cambridge Analytica u ožujku 2018. godine, Facebook je više puta napomenuo da je onemogućio vanjski pristup do korisničkih podataka. Podaci su se dijelili sa 61 proizvođačem softverske i hardverske opreme, ali i s nizom razvojnih programera.
- Kasnije istog mjeseca otkriven je novi trojanski konj koji je jedan u nizu inačica zlonamjernog softvera iz skupine Rakhni, a posjeduje sposobnost biranja načina na koji će djelovati ovisno o konfiguraciji zaraženog računala. Naime, ovaj zlonamjerni program u najnovijoj inačici provjerava žrtvin sustav te temeljem prikupljenih informacija odlučuje hoće li žrtvino računalo kompromitirati zlonamjernim ransomware programom ili će koristiti resurse zaraženog računala za rudarenje kriptovaluta.
- Mađarski CERT sredinom srpnja prijavio je uspješno iskorištavanje propusta u HP management card modulu čime je napadač ostvario pristup sustavu, dodao novog korisnika i pokušao instalirati Windows operacijski sustav. Postoji mogućnost da je incident povezan s drugim incidentima kod koji se iskorištavao HP iLO softver za „rudarenje" kriptovaluta. Slučaj je prijavljen Cyber Crime odjelu pri MUP-u.
- Sredinom mjeseca srpnja otkrivena je botnet mreža koja je izgrađena korištenjem ranjivosti u Huawei HG532 usmjernicima. Botnet mreža je u jednom danu narasla na 18 000 usmjernika, a autor koji je stajao iz mreže javio se sigurnosnim stručnjacima kako bi se pohvalio svojim radom te im je čak i podijelio listu IP adresa žrtava. Autor se predstavio pseudonimom "Anarchy", no vjeruje se da se radi o od prije poznatom zlonamjernom korisniku "Wicked" koji je razvio niz inačica raznih zlonamjernih sadržaja, prvenstveno Mirai IoT botnet.
- Krajem mjeseca zaprimljen je veći broj prijava za ucjenjivačke "scam" poruke e-pošte kojima ucjenjivač pokušava iznuditi novčanu dobit od žrtve. Metoda kojom napadač pokušava ostvariti financijsku dobit temelji se na objavljivanju navodnih osjetljivih podataka žrtve koja je primila ucjenjivačku poruku ako žrtva ne izvrši uplatu u Bitcoin vrijednosti. Nacionalni CERT objavio je sigurnosno upozorenje preko svih komunikacijskih kanala kako bi korisnike uputili u postupke koje je važno poduzeti. Hrvatski korisnici su prijavljivali ucjenjivačke „scam" poruke e-pošte do kraja godine.
- Početkom kolovoza bila je aktivna botnet kampanja u kojoj su se masovno napadali MikroTik usmjerivači. Napadi su iskorištavali ranjivost MikroTik RouterOS za koju je zakrpa izdana još u travnju 2018. godine. Iskorištavanje ranjivosti napadaču omogućava udaljeno čitanje korisničkih imena i lozinki administratorskih računa na usmjerivaču. Napadi u sklopu ove botnet kampanje između ostaloga se koriste i za širenje zlonamjernog softvera za rudarenje kriptovaluta. Botnet kampanja bila je aktivna i u Hrvatskoj te su postojali znakovi da se zaraženi uređaji koriste za slanje neželjene pošte.

- U kolovozu, na DEF CON sigurnosnoj konferenciji, sigurnosni su stručnjaci objavili detalje o 47 ranjivosti unutar ugrađenog softvera (engl. firmware) i tvorničkih aplikacija na 25 Android pametnih telefona. Ranjivosti mogu biti jednostavne greške koje uzrokuju gašenje uređaja, ali i rizični bugovi koji napadačima omogućavaju root pristup uređaju. Neke od ovih ranjivosti omogućavaju napadačima pristup i slanje SMS poruka sa žrtvina uređaja, preuzimanje preslike ekrana, dohvaćanje imenika te preuzimanje i instalaciju aplikacija bez znanja žrtve.
- Početkom rujna avio kompanija British Airways potvrdila je neovlašteno otkrivanje povjerljivih osobnih podataka i brojeva kartica gotovo 380 000 korisnika. U izjavi što ju je British Airways objavio stoji kako su kompromitirani podaci korisnika koji su rezervirali letove putem stranice ba.com i aplikacije British Airways u periodu od 21. kolovoza do 5. rujna.

4. kvartal

- U prvoj polovici listopada, Facebook je nakon što je u rujnu objavio da su ukradeni podaci 90 milijuna korisnika, izjavio kako se ipak radilo o „samo" 30 milijuna korisnika. Djelatnici društvene mreže su pristup podacima onemogućili nakon dva dana. Napadači su iskorištavali funkcionalnost "view as" koju su mnogi korisnici koristili kako bi ustanovili što je na njihovim profilima vidljivo različitim tipovima korisnika. Funkcionalnost je bila privremeno onemogućena.
- Sredinom studenog banke u Rusiji bile su meta masivne phishing kampanje čiji je cilj isporuka zlonamjernog alata kojeg koristi hakerska skupina Silence. Za članove ove grupe se vjeruje da imaju pozadinu u legitimnim poslovima u kibernetičkoj sigurnosti te da imaju pristup dokumentima financijskog sektora. Primjeri zlonamjernih poruka elektroničke pošte odaslani su na adrese Središnje banke Ruske Federacije, a sadržavale su zlonamjerni privitak. U tekstu se poruke tražilo od primatelja da preuzmu i otvore privitak kako bi provjerili detalje o "novim pravilima elektroničke komunikacije unutar tvrtke".
- Krajem studenog velik broj Amazon korisnika zaprimio je poruku elektroničke pošte u kojoj Amazon navodi da je greškom objavio njihovu adresu elektroničke pošte. U trenutku slanja obavijesti poteškoća je otklonjena, a prema dostupnim informacijama bila je uzrokovana poteškoćom u radu web sjedišta.
- Sredinom prosinca Ministarstvo pravosuđa Sjedinjenih Američkih Država (eng. *Justice Department*) objavilo je FBI-evo preuzimanje kontrole nad 15 domena koje su korištene u sklopu "DDoS-for-hire" servisa. Uhićeno je troje pojedinaca koji su i optuženi za održavanje tih servisa. "DDoS-for-hire" servisi dopuštaju zlonamjernom korisniku zakup mreže zaraženih računala te izvođenje DDoS napade putem nje.
- Krajem prosinca bila je aktivna phishing kampanja koja je ciljala korisnike American Express kreditnih kartica. Tekst poruke navodio je korisnike na pokretanje poveznice do phishing stranice zbog "navodnih" problema s njihovom karticom. Na phishing stranici nalazila se online forma u kojoj se od korisnika traži unos povjerljivih osobnih podataka koji između ostalog uključuju bankarske podatke.

7 Zaključak

Tijekom 2018. godine Nacionalni CERT provodio je proaktivne i reaktivne mjere s ciljem smanjenja rizika od pojave računalno-sigurnosnih incidenta i umanjenja štete u slučaju njihovog nastanka. 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.

Nacionalni CERT nastavio je s aktivnostima svog prvog samostalnog projekta sufinanciranog sredstvima Instrumenta za povezivanje Europe pod nazivom GrowCERT. Projektom se doprinosi ispunjenju ciljeva Nacionalne strategije kibernetičke sigurnosti. Provedbom projekta doprinosi se jačanju nacionalnih kapaciteta za prikupljanje, analizu i razmjenu informacija o kibernetičkim incidentima i prijetnjama kibernetičkoj sigurnosti korištenjem novorazvijene platforme za prikupljanje podataka o sigurnosnim incidentima na nacionalnoj i europskoj razini. Projektom se također želi podići svijest o kibernetičkim prijetnjama te adekvatnim odgovorima na iste.

Nacionalni CERT je i tijekom 2018. godine uspješno sudjelovao u NATO-ovoj Cyber Coalition vježbi, gdje je Republika Hrvatska sudjelovala u svojstvu igrača. Vježba, između ostalog, obuhvaća obranu od zlonamjernog sadržaja (eng. *malware*) i hibridne izazove. Testirane su operativne i pravne procedure te suradnja s privatnim sektorom i akademskom zajednicom koji su se i ove godine iskazali kao partneri iz Hrvatske. Vježbom se rukovodilo iz NATO-ovog centra izvrsnosti.

U 2018. Godini Nacionalni CERT sudjelovao je u dvije ENIS-ine vježbe - "Cyber SOPEx" i "Cyber Europe". Cilj vježbe "Cyber SOPEx" je poboljšanje suradnje između CSIRT-ova. Scenarij se temeljio na kibernetičkim napadima na pomorski sektor. Vježbom se, osim suradnje, poticao i kreativni pristup rješavanju računalno-sigurnosnih incidenata. Scenarij vježbe "Cyber Europe" je sadržavao tehničke i netehničke probleme temeljene na stvarnim iskustvima za čije rješavanje je bila potrebna mrežna analiza i analiza zlonamjernog softvera, forenzika i steganografija. Incidenti u scenariju osmišljeni su tako da prerastu u krizu na svim mogućim razinama: organizacijskoj, lokalnoj, nacionalnoj i europskoj.

Sumarno, prema statistikama, može se zaključiti kako razina incidenata koji se odnose na broj registriranih botova konstantno raste što je rezultat dodavanja dva nova izvora iz kojih se povlače podaci. Broj obrađenih prijava koje se mogu klasificirati kao računalno-sigurnosni incidenti u nadležnosti Nacionalnog CERT-a je u padu. To možemo pripisati činjenici o povećanju svijesti korisnika o ugrozama na internetu te većoj vidljivosti Nacionalnog CERT-a u javnosti u odnosu na prethodnu godinu. Posjećenost portala antibot.hr tijekom 2018. godine dosegla je brojku od 55 064 korisnika. Broj otkrivenih kompromitiranih web sjedišta u odnosu na prethodnu godinu smanjio se za 26 %. Najznačajnija promjena u odnosu na prethodnu godinu je rast broja hoax incidenata koji su zauzeli visoko treće mjesto prema tipu, osobito ako uzmemo činjenicu da je "hoax" definiran novom nacionalnom taksonomijom koja se počela primjenjivati od 1. kolovoza 2018. Velika promjena odnosi se i na pad broja web defacement incidenata kojih je u 2018. godini bilo 102 manje nego u 2017. godini.

Zaključno, Nacionalni CERT u 2018. godini ostvario je značajne pomake na području nacionalne i međunarodne suradnje, daljnjeg usavršavanja djelatnika te na području povećanja razine spremnosti na odgovor na sve složenije sigurnosne izazove.

8 Mali pojmovnik računalno-sigurnosnih incidenata

Nacionalni CERT obrađuje incidente ako se jedna od strana uključenih u incident nalazi u .hr domeni ili u hrvatskom IP adresnom prostoru. U nastavku se nalazi kratak opis incidenata koji se spominju u ovom izvještaju.

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

Gdje nas sigurno možete naći?

CERT.hr
surfaj sigurnije

Ovisno o tome kako vam 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**.

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

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

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

2/2019.