POROČILO O KIBERNETSKI VARNOSTI

ZA LETO 2021

si·cert

Nacionalni odzivni center za kibernetsko varnost

Nacionalni odzivni center za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team) opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost.

www.cert.si

Facebook: **facebook.com/sicert**

Twitter: **@sicert**

www.varninainternetu.si

Facebook: **facebook.com/varninainternetu**

Twitter: **@varninanetu**

Instagram: **instagram.com/varninainternetu**

URSIV

Dejavnosti centra SI-CERT financira
Urad Vlade Republike Slovenije
za informacijsko varnost.

Poročilo o kibernetski varnosti 2021

SI-CERT

Nacionalni odzivni center za kibernetsko varnost

KAZALO

UVODNI NAGOVOR

Leto ranljivosti in težav dobavne verige

Že sedaj lahko rečemo, da si bomo v skupnosti odzivnih centrov za kibernetsko varnost (CSIRT) leto 2021 zapomnili po velikem številu razkritih ranljivosti. Obravnava teh spada v običajni nabor dela odzivnih centrov, vendar pa je leto 2021 posebno po tem, da so bile v ospredju ranljivosti dobavne verige (ang. *supply chain*).

Začelo se je že marca 2020 z vdorom v omrežje proizvajalca SolarWinds, ko so storilci namestili stranska vrata v produkt Orion, podjetje pa je to zlonamerno komponento nevede posredovalo svojim strankam ob rednih nadgradnjah. Tako so storilci (po ocenah gre za državno podprte akterje) lahko pridobili dostop do upravljanja naprav končnih uporabnikov, med katerimi so bile številne pomembne organizacije. Do razkritja ranljivosti je prišlo šele proti koncu 2020. Nekaj mesecev pozneje je sledila prva v seriji ranljivosti strežnikov Microsoft Exchange, kjer je bilo hitro ukrepanje pomembno zaradi sorazmerno velike razširjenosti produkta. Eno od spoznanj je, da je pomembna skrb za celoten ekosistem kibernetskega prostora, kjer je veliko majhnih in srednjih podjetij. Tam smo žal lahko spremljali dokaj počasno nameščanje popravkov, enak sklep smo lahko potegnili tudi poleti ob ranljivosti ProxyShell. Leto pa smo zaključili v stanju povečane pripravljenosti celotne mreže Evropske unije CSIRT in ob razglašeni povečani ogroženosti glede varnosti omrežij in informacijskih sistemov (s strani Urada Vlade Republike Slovenije za informacijsko varnost) zaradi 0-day ranljivosti v knjižnici Log4J. Gre za odprtokodno knjižnico, ki pa jo uporablja zelo veliko drugih produktov, veliko je tudi znanih komercialnih imen. Čeprav se ni zgodil internetni armagedon, kot so napovedovali nekateri, pa nam je lansko leto temeljito odprlo oči glede upravljanja kibernetske varnosti pri pospešeni digitalizaciji.

GORAZD BOŽIČ,
vodja SI-CERT

IZPOSTAVLJENI DOGODKI V 2021

- **ranljivosti dobavne verige**
  (izpostavljeni: SolarWinds, MS Exchange, Log4j)
- **smrt in ponovno vstajenje trojanskega konja Emotet**
- **phishing še vedno narašča**
- **predsedovanje mreži skupin CSIRT**
- **Varni v pisarni – brezplačni tečaj o informacijski varnosti za zaposlene**
- **KLIK – nova video serija kratkih dokumentarnih filmov o spletnih goljufijah**
- **10 let programa ozaveščanja Varni na internetu**
  (več na strani 12)

IZSTOPAJOČE ŠTEVILKE V 2021

→ več kot **3.000** obravnavanih incidentov

→ **37**-odstotni porast phishinga

→ več kot **300** obravnavanih primerov zlonamerne kode

→ **104** novinarska vprašanja

NA KRATKO O SI-CERT

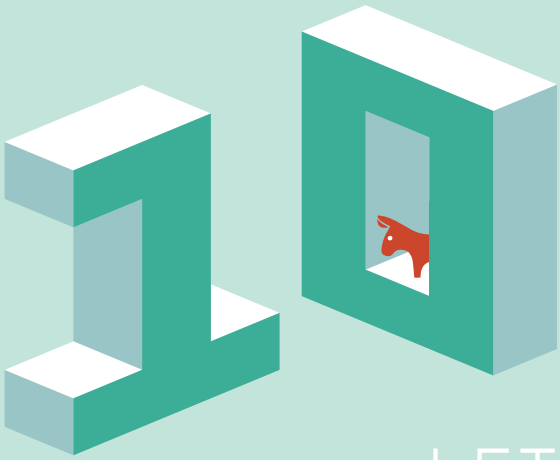
si·cert
Nacionalni odzivni center za kibernetsko varnost

Nacionalni odzivni center za kibernetsko varnost SI-CERT (Slovenian Computer Emergency Response Team) je bil ustanovljen leta 1995. Primarna naloga centra je strokovna pomoč pri preiskovanju incidentov, koordinacija njihovega razreševanja, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdajanje opozoril upraviteljem omrežij in širši javnosti o trenutnih grožnjah v kibernetskem prostoru. SI-CERT izvaja nacionalni program ozaveščanja in izobraževanja *Varni na internetu*.

Delovanje centra SI-CERT opredeljuje 28. člen Zakona o informacijski varnosti (ZInfV). Bogate izkušnje, osredotočenost na specializirana strokovna znanja za preiskovanje računalniških incidentov in dobra mednarodna vpetost postavljajo SI-CERT v središče operativnega delovanja pri odzivanju na kibernetske incidente v državi. Kot nacionalna kontaktna točka imamo vpogled v trende, podatki o sorodnih incidentih doma in v tujini pa izboljšajo in pospešijo razreševanje aktualnih primerov.

Aktivnosti SI-CERT-a financira Urad Vlade Republike Slovenije za informacijsko varnost, ki je pristojni nacionalni organ za kibernetsko varnost.

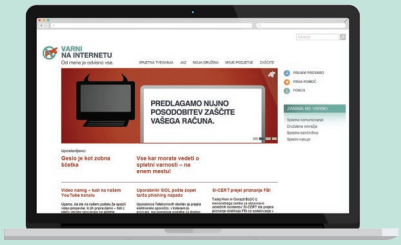
KDAJ PRIJAVITI INCIDENT SI-CERT-u?	KAJ STORIMO?
okužba računalnika: izsiljevalski virusi, bančni trojanski konji, ciljani napadi, agenti za pošiljanje neželene elektronske pošte	pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do sedaj znanimi grožnjami; svetovanje o ukrepih za sanacijo stanja
opažen vdor v strežnik: razobličenje, zloraba podatkovnih baz, namestitev prikritih orodij storilca	iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri ugotavljanju posledic in iskanju vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito
sumljiva elektronska sporočila: sporočila za zvabljanje oz. phishing sporočila, ponudbe za hiter zaslužek ali ugodna posojila	odstranjevanje in označevanje lažnih spletnih mest; prepoznavanje širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev
napad onemogočanja: izredno povečanje prometa oz. poplava s prometom, napad na storitev ali spletno aplikacijo, da se onemogoči njeno delovanje	ocena o uporabljenih sredstvih za napad, opredelitev možnih zaščitnih ukrepov, poskus onemogočanja botneta ter obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti
ranljive ali izpostavljene storitve: vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja	obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve
izguba gesel ali kraja omrežne identitete: zloraba prek phishing napada ali napada prek okužbe računalnika	svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in iskanju storilca
spletna goljufija: lažne spletne trgovine, prevare pri prodaji in nakupih prek spletnih posrednikov, lažna posojila, nigerijske, loterijske in ljubezenske prevare	ocena tveganja, odstranjevanje lažne spletne trgovine s spleta, ozaveščanje javnosti



10 LET NACIONALNEGA PROGRAMA OZAVEŠČANJA **VARNI NA INTERNETU**

2011

VARNI NA INTERNETU
Od mene je odvisno vse.



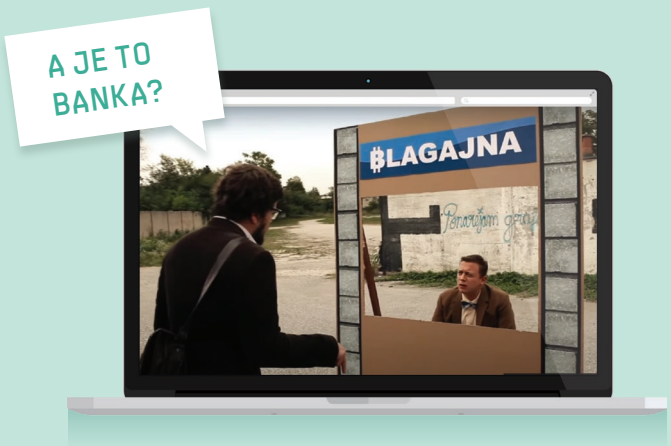
9. februar 2011: novinarska konferenca ob predstavitvi programa ozaveščanja Varni na internetu širši javnosti. Postavimo temelje – nov portal www.varninainternetu.si, kjer so na enem mestu zbrana opozorila o aktualnih prevarah, svetovalni članki, na voljo pa je tudi prijavni obrazec za sporočanje spletnih prevar. Kot najbolj kritična področja identificiramo spletne prevare, krajo identitete in spletno bančništvo. Kako to problematiko predstaviti spletnim uporabnikom? Poglavitno sporočilo projekta ozaveščanja se glasi: »Od mene je odvisno vse.« Sami namreč lahko storimo največ, da zmanjšamo tveganja.

Novembra 2011 naš portal www.varninainternetu.si dobi priznanje netko kot najboljši v kategoriji predstavitve institucij s področij državne in javne uprave.

2012

Slovenija je s programom Varni na internetu ena od devetih članic EU, ki sodeluje v manjšem pilotnem projektu Evropski mesec kibervarnosti. Pobuda bo čez leta vključevala vse članice EU in več kot 300 partnerjev in podpornikov.

Prvič se lotimo video kampanje in pokažemo, da s humornim, pozitivnim pristopom žanjemo več odziva in pozornosti kot s strašenjem spletnih uporabnikov. Test časa bo pokazal, da video »A je to banka?« še vedno nasmeji polno predavalnico. Lahko rečemo, da smo ena prvih družbeno odgovornih kampanj, ki v središče postavi video, komunikacijo na družbenih omrežjih in sodelovanje s prepoznavnimi obrazi, kar je čisto nov pristop, še posebej v svetu informacijske varnosti.



2013

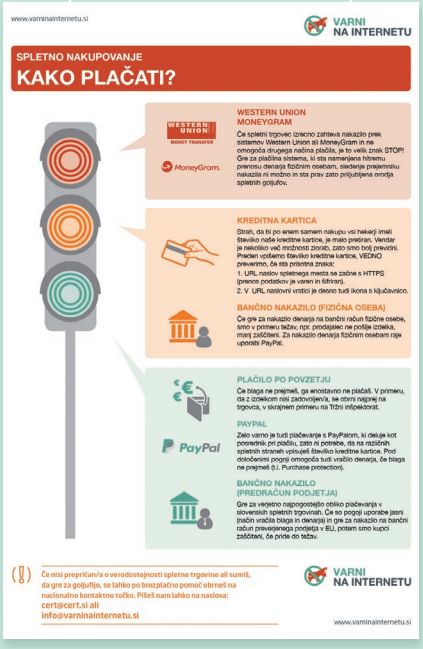
MALI IN VELIKI POMP!

SI-CERT prejme nagradi POMP za najboljše letno poročilo in VELIKI POMP za projekt leta na področju vsebinskega marketinga za program ozaveščanja Varni na internetu.

Izdamo dva pomembna priročnika, ki obravnavata pogosto spregledani problematiki. V sodelovanju z Informacijskim pooblaščencem izdamo priročnik **ABC varnosti in zasebnosti na mobilnih napravah** ter v sodelovanju z nacionalnim registrom za domeno .si pripravimo smernice **ABC varnosti za lastnike spletnih strani**.

2014

Izvedemo Prevarantski tour po Sloveniji. V sklopu kampanje Evropski mesec kibervarnosti zasnujemo spletno kampanjo, ki jo podpremo s turnejo Gledališča Ane Monro. Predstava pokaže, kakšne so videti spletne goljufije, če jih preslikamo v resnični svet.



Oblikujemo in natisnemo prvi plakat, s katerim pojasnjujemo tveganja pri različnih možnostih plačevanja v spletnih trgovinah.

2015

Dosežemo pomemben mejnik – pri SI-CERT-u se prvič zgodi, da število prijavljenih spletnih goljufij preseže število tehničnih incidentov, kar je med drugim tudi posledica izobraževanja o spletni varnosti in delovanja naše prijavne točke.

Na Facebookovi strani Varni na internetu presežemo (takrat magično) mejo 20.000 sledilcev.

Prvič se pridružimo pobudi **Svetovni dan varnostnega kopiranja** (World Backup Day) in opozorimo na hitro širjenje izsiljevalskih virusov. Kot zanimivost – leta 2015 so storilci zahtevali odkupnino v vrednosti od dva do štiri bitcoine, kar je takrat znašalo nekaj manj kot 1.000 evrov.

2016

Leto v znamenju spletnega nakupovanja. Na skupni tiskovni konferenci SI-CERT, Tržni inšpektorat Republike Slovenije, Evropski potrošniški center Slovenija in Javna agencija Republike Slovenije za zdravila in medicinske pripomočke opozorimo na problematiko **goljufij pri spletnem nakupovanju**.

Premierno predstavimo novo video kampanjo, sestavljeno iz štirih video zgodb, med katerimi izstopa Hipster Lovrenc, ki je prek spleta kupoval traktor. Zaradi zanimanja v skupnosti ENISA začnemo z angleškim podnaslavljanjem naših videov.

Na našem kanalu YouTube z video kampanjo zabeležimo več kot 120.000 ogledov v enem mesecu, kar je v tistem času velik uspeh.

2017

Predstavimo novost – Facebookovo video serijo Šol@ preživetja z Jožetom, ki **preseže mejnik 1.000.000 ogledov**. V osmih video blogih na humoren način predstavimo osem najpogostejših spletnih zagat in zabeležimo velik odziv.

Video kampanjo in naše preostale aktivnosti predstavimo Evropski komisiji, kjer prejmemo posebno pohvalo za naš pristop k ozaveščanju o informacijski varnosti.

Prvič nagovorimo tudi podjetja in zaposlene – ob mesecu kibervarnosti 2017 postavimo v ospredje nevarnosti, ki prežijo na manjša podjetja in zaženemo kampanjo Najstrašnejša žival je … miš!

V sodelovanju z Europolom prevedemo in pomagamo pri postavitvi slovenske verzije portala NoMoreRansom.org. Z globalno pobudo **No More Ransom** so žrtvam izsiljevalskih virusov na voljo dešifrirni ključi, ki omogočajo odklep in povrnitev njihovih dokumentov brez plačila.

Skupaj z Odsekom za kibernetsko varnost Slovenske vojske izdamo priročnik **Slovenski vojaki in vojakinje ponosni in varni tudi na spletu**. Pozitivno in proaktivno sodelovanje opazijo tudi v Policiji, tako zasnujemo nov priročnik– **Policistke in policisti, bodite varni na internetu tako doma kot v službi**. Publikacijo natisnemo v nakladi 5.000 izvodov in jo pošljemo vsem policijskim upravam po Sloveniji.

2018

Ob svetovnem dnevu varnostnega kopiranja predstavimo kviz Mit ali resnica? in se prvič lotimo sodelovanja z vplivneži, kar takrat pomeni čisto nov pristop pri komunikaciji s spletnimi uporabniki. Popotnika in pisca bloga sta delila svojo izkušnjo, ko sta izgubila celoten fotografski arhiv, saj nista imela ustrezne varnostne kopije.

Za kampanjo ob mesecu kibervarnosti 2018 Varni ali prevarani prejmemo **nagrado WEBSI za drugo mesto v kategoriji družbeno odgovorni projekt**i. Še eno prelomnico predstavlja dejstvo, da smo prvič sodelovali na evropskem natečaju in tako financirali kampanjo s pomočjo sredstev Instrumenta za povezovanje Evrope (CEF; The Connecting Europe Facilitiy).

2019

Organiziramo okroglo mizo z naslovom »Ljubezenske prevare na spletu«, s katero smo slovensko javnost opozorili na velik porast tovrstnih prevar.

Predstavništvo Evropske komisije v Sloveniji nas je povabilo k sodelovanju v kampanji »EU protects« oz. »**EU varujemo skupaj**«, s katero Evropska unija opozarja na zgodbe posameznikov, ki s svojim delom dnevno skrbijo za zaščito ljudi v Evropi.

2020

Program Varni na internetu prejme slovensko veliko nagrado varnosti 2020, in sicer za najboljši strokovni prispevek s področja korporativne varnosti. **Slovenska velika nagrada varnosti je najvišja nagrada s področja varnosti v Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti**. Nagrado v šestih kategorijah podeljuje Inštitut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti.

Še naprej širimo svoje aktivnosti in vzpostavimo nov kanal – Instagram račun Varni na internetu, saj želimo tako doseči predvsem mlajši del ciljne populacije.

Na naši Facebookovi strani presežemo 40.000 sledilcev.

SI-CERT za svoja prizadevanja prejme **nagrado ambasador zasebnosti, ki jo podeljuje Informacijski pooblaščenec**. Izpostavijo naš program Varni na internetu, ki pomaga tako posameznikom kot organizacijam k varni uporabi sodobnih tehnologij, s tem pa dviga tudi ozaveščenost o varstvu osebnih podatkov in zasebnosti.

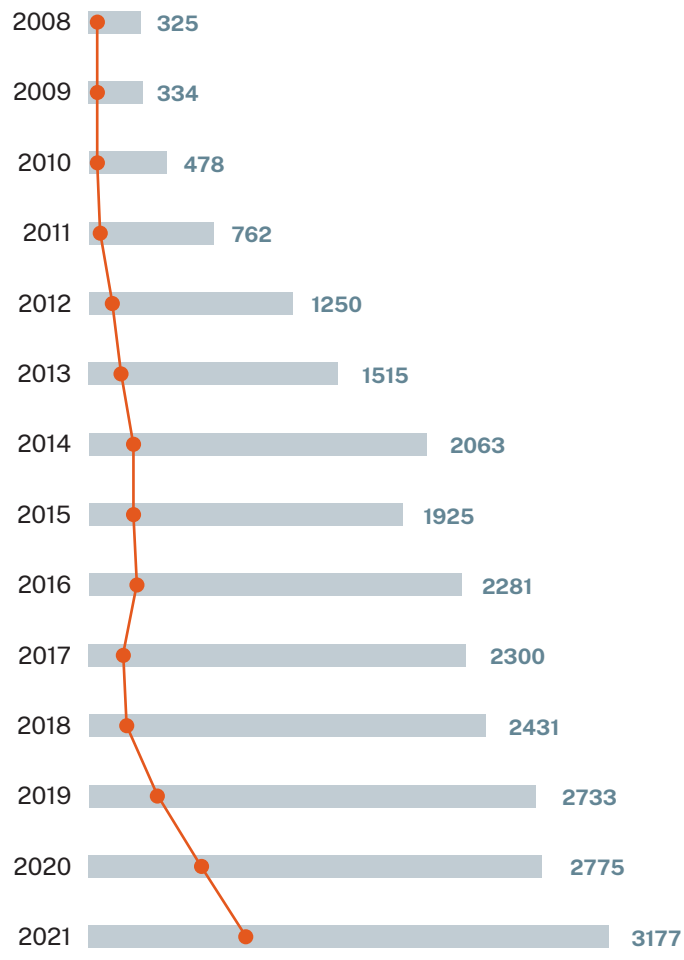
Prenovljeni portal www.varninainternetu.si osvoji še eno nagrado netko, in sicer za 1. mesto v kategoriji **Naj spletna stran za družbeno odgovornost**.

KLJUČNI KAZALCI IN STATISTIČNI PREGLED

POJAVNOST KLJUČNIH BESED
V OBRAVNAVANIH INCIDENTIH

ŠTEVILO INCIDENTOV V LETIH 2008–2021
S POUDARKOM NA PHISHING PREVARAH

Leto	Incidentov	razlika (%)	Phishing	% phishinga
2008	**325**		23	7,08 %
2009	**334**	2,77 %	38	11,38 %
2010	**478**	43,11 %	50	10,46 %
2011	**762**	59,41 %	61	8,01 %
2012	**1250**	64,04 %	139	11,12 %
2013	**1515**	21,20 %	209	13,80 %
2014	**2063**	36,17 %	279	13,52 %
2015	**1925**	–6,69 %	283	14,70 %
2016	**2281**	18,49 %	296	12,98 %
2017	**2300**	0,83 %	222	9,65 %
2018	**2431**	5,70 %	224	9,21 %
2019	**2733**	12,42 %	435	15,92 %
2020	**2775**	1,54 %	694	25,01 %
2021	**3177**	14,49 %	950	29,90 %



VRSTE IN ŠTEVILO INCIDENTOV
V LETIH 2018–2021

Skupina	Vrsta incidenta	2018	2019	2020	2021
NEPRIMERNA VSEBINA	neželena sporočila	98	57	72	120
	žaljiva vsebina	0	9	22	13
	nasilna vsebina	0	1	3	0
ZLONAMERNA KODA	virus	111	53	46	29
	črv	0	0	0	2
	trojanski konj	73	166	141	171
	vohunska programska oprema	0	3	1	2
	samodejni izbirnik (ang. Dialler)	0	0	0	0
	korenski komplet (ang. Rootkit)	0	0	1	0
	boti in botneti	17	17	16	9
	nadzorni strežnik	0	6	7	0
	izsiljevalski virus	64	53	69	64
	orodje za oddaljeni nadzor (RAT)	5	6	14	29
ZBIRANJE INFORMACIJ	odkrivanje potencialnih tarč in ranljivosti (skeniranje)	75	33	28	41
	prestrezanje komunikacije	0	5	1	1
	socialni inženiring	0	2	2	0
POSKUSI VDORA	izkoriščanje znane ranljivosti	0	5	4	1
	poskusi prijav, napad z grobo silo (ang. Brute Force Attack) in napadi s slovarjem	0	46	16	32
	nova vrsta napada	0	0	0	0
VDORI	zloraba privilegiranega uporabniškega računa	42	6	7	6
	zloraba neprivilegiranega uporabniškega računa	62	35	82	105
	napad na aplikacijo	13	4	4	5

*** NOVINARSKA VPRAŠANJA**
V tabeli Vrste in število incidentov v letih 2018-2021 je razviden velik upad novinarskih vprašanj, ki pa je samo navidezen in je posledica tega, da smo v začetku leta 2021 spremenili njihovo obravnavo: **uvedli smo naslov press@cert.si in ločeno linijo za odgovore**. Skupaj smo (vključno z devetimi spodaj navedenimi) **v letu 2021 prejeli 104 novinarska vprašanja**.

Skupina	Vrsta incidenta	2018	2019	2020	2021
RAZPOLOŽLJIVOST	napad onemogočanja	0	2	7	6
	porazdeljen napad onemogočanja	22	31	31	27
	sabotaža	0	4	0	0
	izpad delovanja naprav ali omrežja	0	3	2	4
VARNOST INFORMACIJSKIH VIROV	nepooblaščen dostop do podatkov	0	15	13	12
	nepooblaščeno spreminjanje podatkov	0	5	8	22
	odtekanje informacij	0	4	5	6
GOLJUFIJE	nepooblaščeno izkoriščanje virov	13	8	4	5
	intelektualna lastnina in avtorske pravice	8	13	10	10
	kraja identitete	62	96	67	68
	phishing sporočilo	175	301	488	765
	phishing spletno mesto	47	134	202	185
	spletno nakupovanje	339	164	97	86
	goljufija z vnaprejšnjim plačilom	161	149	168	182
	izsiljevanje	359	291	144	138
	druge goljufije	341	684	668	655
RANLJIVOSTI	odgovorno razkrivanje	5	25	14	12
	razkritje ranljivosti	0	1	2	12
	ranljivi sistemi in naprave	0	24	20	33
DRUGO	drugo	246	243	226	301
	novinarsko vprašanje*	**47**	**17**	**53**	**9**
TEST	namenjeno preizkusom	0	3	1	1
Skupaj		2385	2724	2766	3169
Nerazvrščenih		46	9	9	8
Vseh primerov skupaj		**2431**	**2733**	**2775**	**3177**

ŠTEVILO INCIDENTOV PO SKUPINAH
V LETIH 2018–2021

Skupina	2018	2019	2020	2021
NEPRIMERNA VSEBINA	98	67	97	133
ZLONAMERNA KODA	270	304	295	306
ZBIRANJE INFORMACIJ	75	40	31	42
POSKUSI VDORA	0	51	20	33
VDORI	117	45	93	116
RAZPOLOŽLJIVOST	22	40	40	37
VARNOST INFORMACIJSKIH VIROV	0	24	26	40
GOLJUFIJE (BREZ PHISHINGA)	1283	1405	1158	1144
PHISHING	222	435	690	950
RANLJIVOSTI	5	50	36	57
DRUGO	293	260	279	310

Opomba: primeri, ki jih v SI-CERT-u obravnavamo pod »Drugo«, so večinoma splošna vprašanja, ki se nanašajo na področje informacijske varnosti, in ne prijave incidentov.

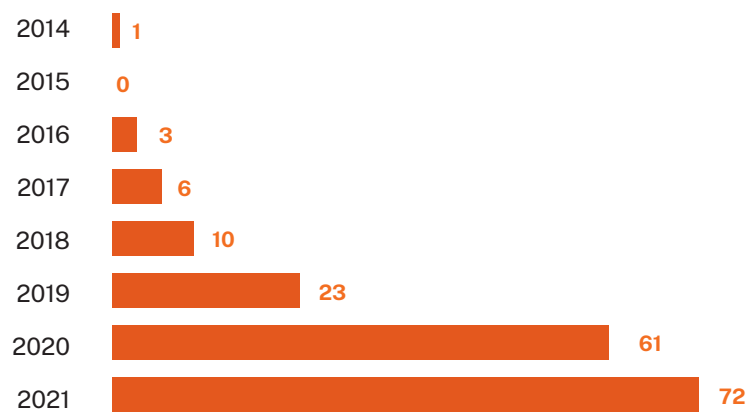
STATISTIKA OŠKODOVANJ

SI-CERT beleži tudi neposredna oškodovanja ob prijavi incidenta, vendar le na podlagi prostovoljne priglasitve prijavitelja. Skupaj je bilo v letu 2021 zabeleženih 166 oškodovanj v incidentih (kar je le nekaj več kot 5 % vseh obravnavanih incidentov). Skupna vsota za samo te incidente je 1,45 milijona evrov. Prijavitelji najpogosteje navedejo oškodovanje ob zlorabah pri spletnem nakupovanju (v 42 % primerov sporočenih oškodovanj), zelo redko pa v primerih izsiljevanja z intimnimi posnetki (le v 3 %).

Vrsta zlorabe	Povprečno oškodovanje
Spletno nakupovanje	1.900 €
Prevara z vnaprejšnjim plačilom (nigerijska prevara)	9.600 €
Investicijske goljufije	28.100 €
Vrivanje v poslovno komunikacijo (BEC)	45.400 €
Ljubezenska prevara	17.000 €
Povprečno oškodovanje za vse vrste zlorab	8.800 €

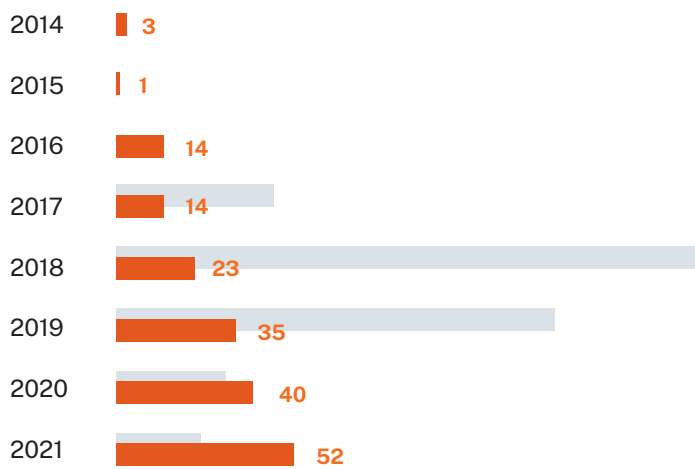
Leto	Število investicijskih prevar
2014	1
2015	0
2016	3
2017	6
2018	10
2019	23
2020	61
2021	72

Investicijske prevare (večinoma lažna vlaganja v kriptovalute)



Napadi na podjetja se nadaljujejo: direktorska prevara (CEO Fraud) upada, zelo verjetno zaradi lahke prepoznavnosti in zato premajhnega izkupička za storilce. Vrivanje v poslovno komunikacijo (BEC, Business Email Compromise) pa narašča, kar kaže na uspešnost tega pristopa, kjer storilci z vdorom v poštni predal spremljajo komunikacijo v podjetju in ob prodaji ali nakupu vskočijo s transakcijskim računom denarne mule in preusmerijo denar.

leto	BEC	CEO Fraud
2014	3	
2015	1	
2016	14	
2017	14	46
2018	23	170
2019	35	128
2020	40	32
2021	52	25



POMEMBNEJŠI INCIDENTI IN OPAŽANJA

RANLJIVOSTI DOBAVNE VERIGE

Ranljivost je niz različnih pogojev, ki omogočajo kršitev varnostne politike. Gre za pomanjkljivosti v informacijskem sistemu, aplikacijah, omrežnih napravah, varnostnih postopkih sistema, notranjem nadzoru ali izvajanju postopkov, ki so lahko predmet izkoriščanja ali zlorabe. Ranljivost lahko povzročijo napake v programski opremi, napačna konfiguracija ali nepričakovane interakcije med različnimi sistemi. Uspešno izkoriščanje ranljivosti ima lahko za posledico tehnična tveganja in tudi tveganja, ki lahko ogrozijo celoten sistem. Skoraj celotna panoga proizvajalcev digitalnih rešitev je sprejela model *odgovornega* ali *koordiniranega razkrivanja ranljivosti,* s katerim se zmanjša škodljiv vpliv ranljivosti na prizadete uporabnike. Med razkrivanjem informacij o varnostnih ranljivostih različni deležniki včasih sledijo nepisanim pravilom ali neformalnim smernicam o medsebojnem povezovanju in izmenjavi informacij.

SOLARWINDS

Marca 2020 je prišlo do vdora v podjetje SolarWinds, med katerim so storilci namestili stranska vrata v platformo Orion za upravljanje naprav, podjetje pa je to zlonamerno komponento nevede posredovalo svojim strankam ob rednih nadgradnjah. Kot kaže, je to omogočilo nadaljnje vdore v eno vodilnih podjetij na področju kibernetske varnosti FireEye in celo v ministrstvo za domovinsko varnost ZDA. Vdor je bil razkrit šele decembra 2020, preiskava SI-CERT-a januarja 2021 pa je pokazala zelo majhno razširjenost platforme SolarWinds Orion v Sloveniji, pri posameznih namestitvah pa smo nato ocenjevali možnost, da ta vsebuje zlonamerno komponento. Tega v nobenem primeru nismo mogli potrditi, zato menimo, da vdor v SolarWinds ni imel konkretnih posledic za omrežja v Sloveniji.

KOORDINIRANO RAZKRIVANJE RANLJIVOSTI
Koordinirano razkrivanje ranljivosti je znano tudi kot odgovorno, delno ali omejeno razkrivanje, pri katerem varnostni raziskovalec odkrito ranljivost sam ali prek posrednika sporoči razvijalcu, nato ta varnostno vrzel odpravi, nazadnje pa se ranljivost razkrije javnosti.

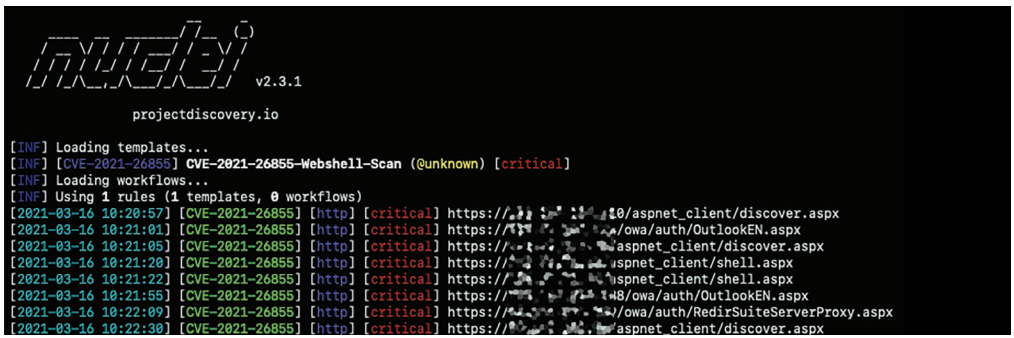
V lastno razvitih aplikacijah lahko ranljivosti odpravimo s popravki sami (oziroma to opravi razvijalec aplikacije), medtem ko smo pri ranljivostih kupljenih naprav in programske opreme večinoma odvisni od popravkov, ki jih objavi proizvajalec (takrat govorimo o ranljivostih dobavne verige). Proizvajalec opreme vedno potrebuje določen čas za pripravo in testiranje popravkov, zato od razkritja ranljivosti do uradnega popravka lahko mine precej časa. Če se ranljivost izkorišča v napadih, še preden je znana proizvajalcu, govorimo o ranljivosti ničtega dne oz. 0-day ranljivosti.

MICROSOFT EXCHANGE

Microsoft je 3. marca 2021 ob 06:35 po srednjeevropskem času (v Seattlu je bil takrat še 2. marec) objavil opozorilo o več kritičnih ranljivostih njihovega strežnika Exchange (ProxyLogon). Šlo je za več 0-day ranljivosti, kar pomeni, da so bile znane (in tudi izkoriščane) v omrežju, še preden je za to vedel Microsoft in vsekakor še preden so bili na voljo popravki. To je pomenilo, da so bili v tistem trenutku vsi strežniki Exchange izpostavljeni potencialnim napadom in podtikanjem stranskih vrat. Pri SI-CERT-u smo objavili obvestilo še isti dan (SI-CERT obvestilo 2021-01). Podatki o številu strežnikov Exchange v Sloveniji iz drugih dostopnih virov so se nam zdeli nekoliko nizki, zato smo se odločili, da bomo opravili pregled slovenskega internetnega prostora tudi sami. Ta je bil neinvaziven in nam je omogočil identifikacijo ranljivih strežnikov. Izvedli smo nekaj ponovljenih obveščanj skrbnikov še vedno ranljivih strežnikov in jih opozorili na nujnost namestitve varnostnih popravkov.

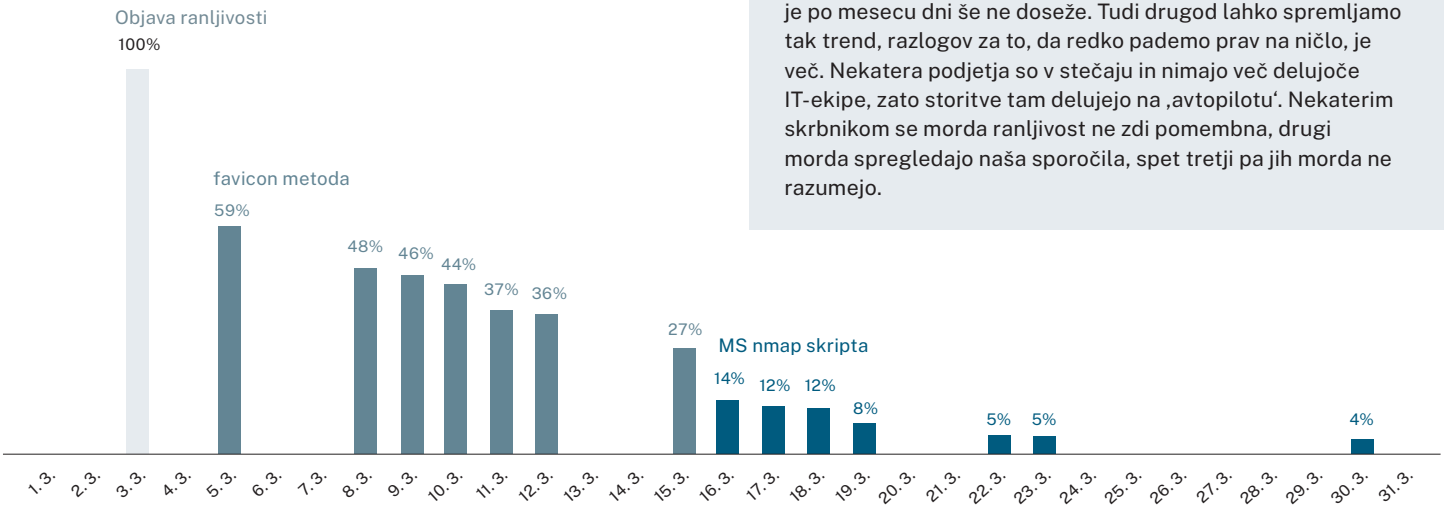
ProxyLogon, **ProxyShell** in **ProxyToken** so 0-day ranljivosti Microsoftovega produkta Exchange, ki so bile razkrite v letu 2021.

Marca 2021 je bilo v Sloveniji 1000 prosto dostopnih strežnikov Exchange.



Iskanje uspešno zlorabljenih strežnikov v Sloveniji s preverjanjem nameščenih stranskih vrat

Spremljanje deleža ranljivih strežnikov MS Exchange v SI-CERT-u marca 2021



DOLGI REP RANLJIVOSTI

Na prikazu padanja deleža ranljivih strežnikov MS Exchange v Sloveniji lahko opazimo, kako se ta delež bliža ničli, vendar je po mesecu dni še ne doseže. Tudi drugod lahko spremljamo tak trend, razlogov za to, da redko pademo prav na ničlo, je več. Nekatera podjetja so v stečaju in nimajo več delujoče IT-ekipe, zato storitve tam delujejo na ‚avtopilotu'. Nekaterim skrbnikom se morda ranljivost ne zdi pomembna, drugi morda spregledajo naša sporočila, spet tretji pa jih morda ne razumejo.

RANLJIVI TUDI POŠTNI STREŽNIKI EXIM

Maja 2021 je bila razkrita vrsta kritičnih ranljivosti poštnega strežnika Exim, ki je priljubljen pri ponudnikih gostovanja. 69 skrbnikov strežnikov v Sloveniji smo opozorili na potrebo po nadgradnji.

18. avgusta 2021 smo o novi verigi ranljivosti (ProxyShell) s podobno akcijo obvestili skrbnike 88 avtonomnih sistemov (AS) v Sloveniji glede potencialno ranljivih namestitev strežnikov Exchange na njihovih omrežjih. Teh je bilo 526.

KASEYA

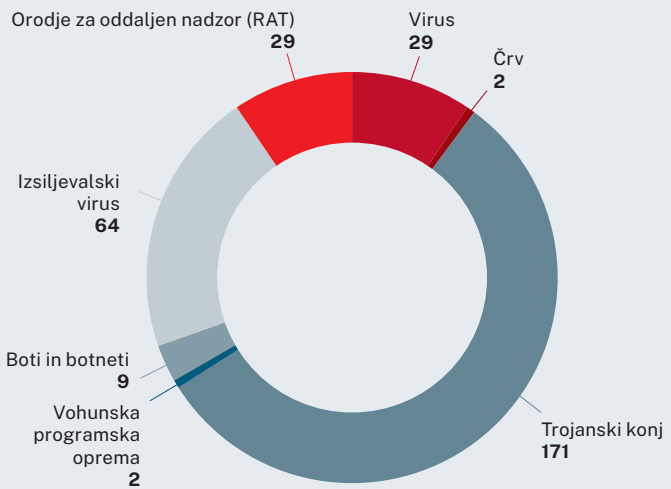
2. julija 2021 se je začel odvijati najobsežnejši napad z izsiljevalsko programsko opremo (ransomware), ki ga je izvedla kriminalna združba REvil. Uporabili so 0-day ranljivost (CVE-2021-30116) v platformi za upravljanje virov IKT ameriškega podjetja Kaseya. Čeprav je najprej kazalo, da gre za še enega v vrsti napadov na dobavno verigo (supply chain attack), v podjetju trdijo, da sami niso bili zlorabljeni za vrivanje škodljive kode, temveč so napadalci neposredno napadli stranke z nameščenimi strežniki Kaseya VSA. Ker gre v veliko primerih za podjetja, ki infrastrukturo ponujajo svojim strankam (MSP, Managed Service Providers), je potencialno število prizadetih žrtev lahko dokaj visoko. V Sloveniji pri SI-CERT-u v letu 2021 nismo prejeli prijave incidenta, povezanega z ranljivostjo Kaseya. Napad je bil sprožen 4. julija ob podaljšanem vikendu v ZDA, ko zaznamujejo praznik neodvisnosti.

LOG4J

Kritična ranljivost knjižnice Log4j, razkrita decembra 2021, je omogočala napadalcu zagon poljubne programske kode na ranljivem sistemu (RCE – Remote Code Execution). Ranljivost se sproži ob zapisu podatka v dnevnik in se lahko izrablja tudi na sistemih, ki niso javno dostopni v internetu, vendar do njih vodi ustrezna podatkovna pot iz javnega dela interneta (tipičen primer je Elasticsearch). Pri obravnavi ranljivosti je bilo treba na to večkrat opozoriti, saj je bila prva reakcija marsikaterega skrbnika v skladu s siceršnjim razmišljanjem glede možnosti za izkoriščanje ranljivosti, a to je bilo tokrat napačno. Ranljivost je bila razširjena tako v odprtokodnih aplikacijah, lastno razvitih rešitvah kot v številnih komercialnih produktih. Identifikacija vseh ranljivih komponent je bila zahtevna in dolgotrajna, univerzalne rešitve za različne postavitve sistemov ni bilo.

ZLONAMERNA KODA

Vrste zlonamerne kode v 2021, obravnavane na SI-CERT



V 2021 smo največkrat obravnavali *trojanske konje;* podtaknjeno zlonamerno kodo, ki se najpogosteje širi v obliki priponk elektronske pošte s sporočili, ki želijo naslovnika prepričati, da nanjo klikne in jo s tem nevede namesti na računalnik. Trojanski konji običajno predstavljajo prvi korak pri nepooblaščenem dostopu do omrežja podjetja skozi okužbo računalnika zaposlenega. Ta ima namreč dostop do marsikaterega vira: internih spletnih aplikacij, diskov v skupni rabi, VPN-dostopa in morda celo do administratorskih vmesnikov za omrežne naprave in domenskih krmilnikov. V naslednjem koraku lahko storilci to izkoristijo za širjenje po omrežju in namestitev izsiljevalskih virusov.

TROJANSKI KONJI IN RAT

Večji del obravnavane škodljive kode so predstavljali trojanski konji za oddaljen dostop (RAT, Remote Access Trojan) in krajo informacij z okuženega računalnika (information stealer trojan). Med zadnjimi je – predvsem zaradi načina širjenja prek ukradenih elektronskih sporočil – prednjačil trojanski konj Emotet, namenjen kraji uporabniških podatkov in gesel. Začetek leta 2021 je zaznamovala uspešna Europolova mednarodno usklajena akcija, s katero so uspeli onesposobiti večji del infrastrukture Emotet. Ob ‚smrti' Emoteta pa je zagon začel pridobivati modularni trojanski konj QBot (SI-CERT obvestilo 2021-03), ki je, enako kot Emotet, imel zmožnost širjenja s pomočjo ukradenih elektronskih sporočil. Ob tem so analize kazale, da za svoje delovanje uporablja del infrastrukture, ki smo jo do takrat pripisovali Emotetu. Z novembrom 2021 smo spet lahko opazovali ponovni zagon in širjenje izvornega Emoteta.

Med škodljivo kodo, ki smo jo v letu 2021 obravnavali v SI-CERT-u, velja omeniti še zaton trojanskega konja FormBook, ki je svoje življenje sicer začel kot preprost beležnik tipkanja oz. keylogger, so pa se njegove zmogljivosti hitro povečevale in ga spremenile v čisto pravega trojanskega konja za krajo podatkov z zmožnostjo kraje gesel iz različnih spletnih brskalnikov, zajemanja zaslonskih posnetkov, spremljanja in beleženja pritiskov na tipkovnici ter prenosa in izvedbe dodatne škodljive kode v skladu z ukazi, ki jih prejema z nadzornega strežnika. Zaton FormBooka pa ni trajal dolgo, saj

je ta na novo zaživel kot XLoader, ki ima sposobnost delovanja tudi v operacijskem sistemu macOS.

Med zanimivejšimi vzorci obravnavane škodljive kode pa velja spomniti na trojanskega konja za krajo podatkov AgentTesla (SI-CERT TZ012 tehnični zapis), ki izstopa predvsem zaradi uporabe širokega spektra načinov za eksfiltracijo ukradenih podatkov iz okuženih sistemov. To stori z uporabo protokola za prenos datotek (FTP), prek elektronskih sporočil (SMTP) ali prek zahtev HTTP POST, pri čemer lahko komunikacijo prikrije z uporabo anonimizacijskega omrežja Tor, ali pa prek aplikacije za hipno sporočanje Telegram.

IZSILJEVALSKI VIRUSI

V obdobju 2016–2019 se je večina napadov z izsiljevalskimi kripto virusi preselila od domačih uporabnikov k bolj ciljanim napadom na podjetja, saj lahko tam napadalci računajo na večje zneske odkupnine. Pred zašifriranjem datotek napadalci ocenijo vrednost podatkov in tako določijo znesek odkupnine za šifrirni ključ. Zneski odkupnine se gibljejo od nekaj sto tisoč do nekaj milijonov evrov, odvisno od velikosti podjetja. Izsiljevanje običajno vsebuje tudi grožnjo z javno objavo ukradenih osebnih podatkov in drugih občutljivih informacij. V 2021 smo mesečno obravnavali nekaj več kot pet prijav okužb z izsiljevalskimi virusi. Glavna vstopna vektorja sta še vedno škodljive priponke v elektronski pošti in neprimerno zaščiten oddaljen dostop do omrežja podjetja (največkrat gre za Windows RDP, v nekaterih primerih tudi za okužbo računalnika zaposlenega in ukradene avtentikacijske podatke za VPN-dostop).

SI-CERT KOT PARTNER EUROPOLOVEGA PROJEKTA nomoreransom.org

Leta 2016 je SI-CERT postal podporni partner projekta nomoreransom.org, ki je pobuda nacionalne enote za visokotehnološki kriminal pri nizozemski policiji, Europolovega centra za računalniški kriminal ter podjetij Kaspersky in McAfee. Cilj pobude je pomagati žrtvam izsiljevalskih virusov, da znova pridobijo dostop do zašifriranih podatkov brez plačila odkupnine napadalcem.

PHISHING

Phishing ali ribarjenje za podatki je vrsta napada z lažnim predstavljanjem, največkrat v elektronskih sporočilih, ki poskušajo prejemnika prepričati v razkritje občutljivih podatkov. Najpogostejši cilji napadov so gesla za elektronsko pošto, prijavni podatki za spletne banke in podatki o kreditnih karticah. Phishing sporočilo prejemnika nagovarja h kliku na povezavo v sporočilu, običajno pod krinko nepredvidenega dogodka, ki terja hitro ukrepanje. Povezava vodi na lažno spletno stran, ki zahteva vpis uporabniškega imena, gesla in drugih osebnih podatkov. Sporočilo in spletna stran ponavadi vsebujeta grafične elemente in podobo ciljane storitve. Nekatere organizacije med phishing uvrščajo tudi druge vrste napadov, npr. elektronsko sporočilo z okuženo priponko ali vabo v SMS klube, pri SI-CERT-u in večini drugih sorodnih organizacij pa je kategorija phishing incidentov omejena zgolj na neposreden poskus kraje osebnih podatkov. V največ primerih je vektor napada elektronska pošta, vedno več napadov z zvabljanjem pa je zaznanih prek SMS-ov in drugih zasebnih sporočil.

Ob zaznavi phishing napada v SI-CERT-u izvedemo različne ukrepe, s katerimi poskušamo napad zaustaviti ali ga omejiti.

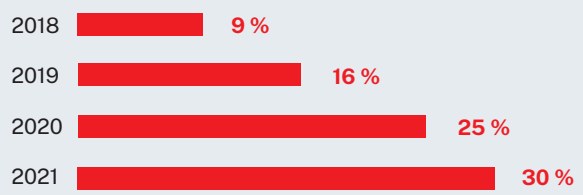
Med temi ukrepi so lahko:

- uvrstitev phishing spletnega mesta na različne zadrževalne sezname (t.i. blackliste)
- obveščanje ponudnika gostovanja spletne strani oz. domene,
- obveščanje drugih deležnikov v Sloveniji in tujini,
- obveščanje javnosti,
- obveščanje posameznih žrtev napada.

Rast phishing napadov

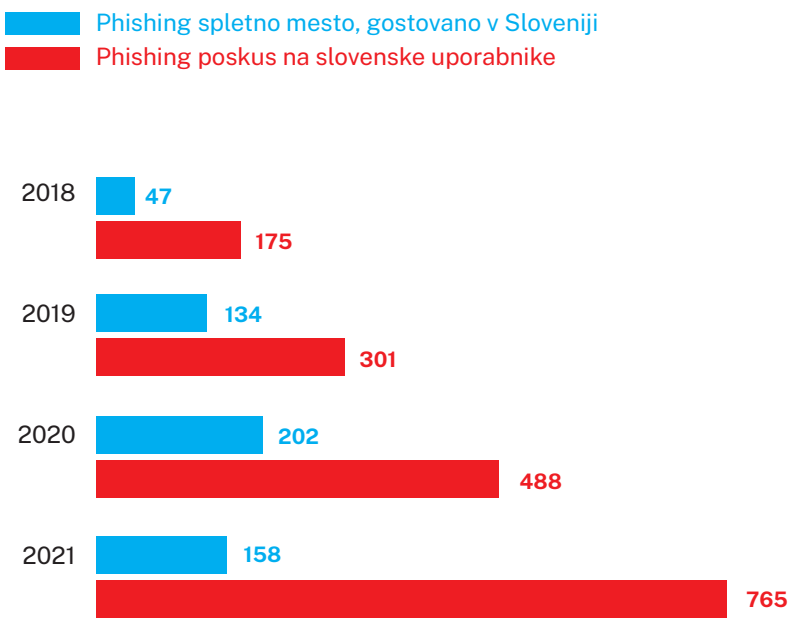
Število obravnavanih phishing incidentov zadnja leta vztrajno raste. Še leta 2018 je število vseh obravnavanih phishing primerov predstavljajo približno 9% vseh obravnavanih

DELEŽ PHISHINGA MED VSEMI OBRAVNAVANIMI INCIDENTI

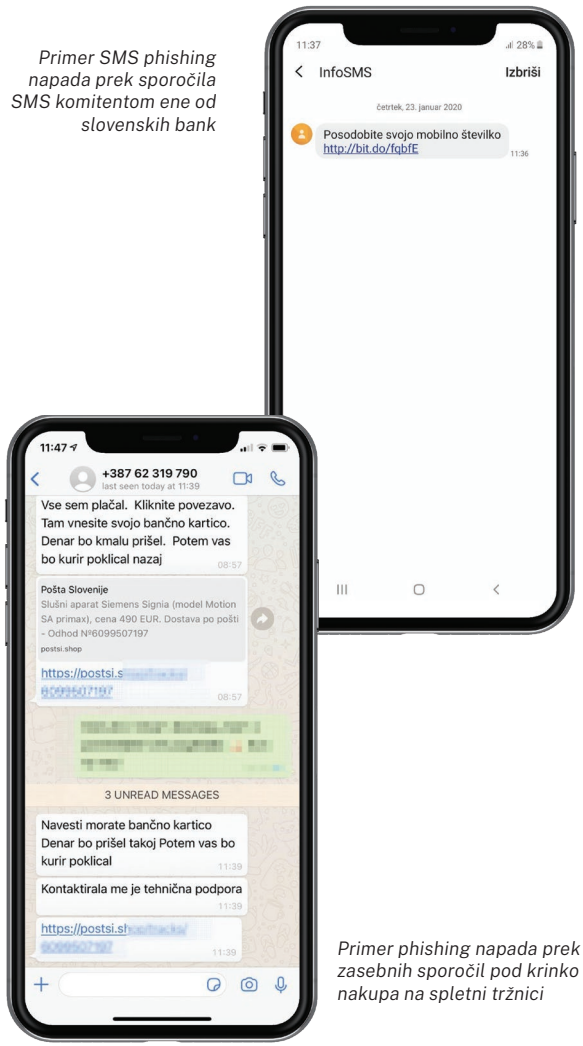


incidentov, leta 2021 pa je ta odstotek dosegel 30 %. Čeprav so phishing napadi ena najstarejših vrst spletnih napadov ter so tehnično povsem enostavni in večinoma temeljijo zgolj na družbenem inženiringu, so še vedno relativno uspešni. Po podatkih SI-CERT-a določen del prejemnikov lažnih sporočil ne prepozna napada in na lažni strani vpiše svoje podatke, kar daje napadalcem motiv za nadaljnje napade.

Število obravnavanih phishing incidentov



Primer SMS phishing napada prek sporočila SMS komitentom ene od slovenskih bank

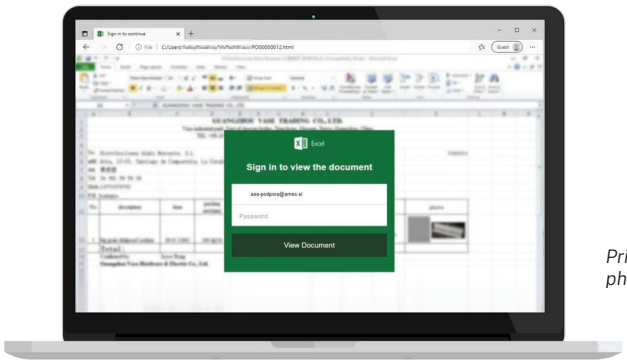


Primer phishing napada prek zasebnih sporočil pod krinko nakupa na spletni tržnici

PHISHING BREZ GOSTOVANJA

Phishing spletne strani so običajno na zlorabljenih spletnih strežnikih ali pa napadalci za gostovanje zlorabijo legitimne storitve, npr. spletne ankete, spletne pisarniške aplikacije, ponudnike brezplačnega gostovanja ipd. Take spletne strani se lahko precej hitro uvrsti na zadrževalne sezname, ki jih uporabljajo spletni brskalniki, poteg tega se večina ponudnikov storitev zaveda problematike in lažne strani po ustaljenih postopkih precej hitro odstranijo. S temi ukrepi je mogoče napad v celoti zaustaviti in onemogočiti.

V letu 2021 smo zaznali povečanje števila phishing napadov, pri katerih sporočila niso vsebovala povezave na lažno spletno stran, ampak je bila ta priložena sporočilom v obliki dokumenta html. Ker lažna stran ni nikjer gostovana, ampak se zgenerira zgolj lokalno v brskalniku, je ni možno blokirati prek zadrževalnih seznamov ali prijave ponudniku gostovanja. Podatki, vpisani v obrazec, se običajno pošljejo prek zahtevka POST na določeno skripto PHP na oddaljenem spletnem strežniku.



Primer lokalne phishing strani

RAZKRITJE FACEBOOKOVIH PODATKOV

Na hekerskih forumih je bila aprila 2021 objavljena zbirka podatkov o 533 milijonih uporabnikov družbenega omrežja Facebook. Podatki so vsebovali ime uporabnika, spol, telefonsko številko in številko profila na omrežju Facebook, kot kaže pa tudi datum zajema podatkov o uporabniku. Ponekod so podatki vsebovali tudi mesto prebivanja, ime delodajalca, status osebnega razmerja, naslov elektronske pošte in rojstni datum. Nekateri od teh podatkov, z izjemo telefonske številke, so bili morda tudi sicer javno dostopni drugim uporabnikom Facebooka, odvisno od nastavitev uporabnikovega profila. Med podatki je bilo tudi 110.177 številk slovenskih uporabnikov. Podatki so lahko koristni različnim storilcem pri izvajanju poskusov goljufij z družbenim inženiringom, incident pa je bil deležen precejšnje medijske pozornosti.

VAJE ZA KIBERNETSKO VARNOST

NATOVA VAJA
LOCKED SHIELDS 21

Slovenija je 2021 prvič sodelovala v Natovi vaji Locked Shields. Ta deluje po načelu »Capture the Flag«, kjer se modre ekipe branijo pred napadi rdeče ekipe. Napadi se odvijajo v skladu z vnaprej pripravljenim scenarijem, ki vključuje tudi širši geopolitični okvir. Slovenija je prvič sodelovala v vaji Locked Shields 21 kot modra ekipa, organizacijo je vodilo Ministrstvo za obrambo Republike Slovenije v sodelovanju s Sekcijo za kibernetsko varnost Gospodarske zbornice Slovenije. SI-CERT je na vaji sodeloval v sklopu strateškega odločanja.

NATOVA VAJA
CYBER COALITION 21

Vaja Cyber Coalition je vodilna vaja zveze NATO in je ena največjih na svetu. SI-CERT od leta 2013 naprej pri tej vaji sodeluje kot igralec. Organizira jo Ministrstvo za obrambo Republike Slovenije. Na vaji se preizkušajo organizacijski in komunikacijski postopki odzivanja na incidente ter zmogljivosti preiskovanja in tehnične analize igral. Ta so običajno vzorci zlonamerne kode in slike zlorabljenih sistemov, na katerih je treba opraviti forenzični pregled.

PROGRAM OZAVEŠČANJA

NACIONALNI PROGRAM OZAVEŠČANJA O INFORMACIJSKI VARNOSTI
VARNI NA INTERNETU

Ozadje programa in njegovi cilji

Varni na internetu je nacionalni program ozaveščanja o kibernetski varnosti, ki slovenske uporabnike že več kot deset let izobražuje o pasteh v spletu.

Program, ki je namenjen najširši javnosti, pokriva ključne probleme: okužbe z zlonamerno kodo, vdore v uporabniške račune, lažne spletne trgovine in trgovine s ponaredki, različne oblike spletnih goljufij, phishing kraje gesel ...

Zaupanje v programske rešitve nas pred takšnimi zlorabami ne obvaruje – edina rešitev je izobraževanje spletnih uporabnikov. Pri tem igra ključno vlogo portal www.varninainternetu.si, kjer je dostopnih več kot 500 svetovalnih člankov s področja informacijske varnosti in opozoril o spletnih goljufijah. Pri obveščanju o aktualnih spletnih prevarah in nevarnostih so pomembni tudi novičnik »Varne novice« ter družbena omrežja Facebook, Instagram in Twitter. **Na naših kanalih praktično vsakodnevno objavljamo vsebine (nasvete in opozorila) in odgovarjamo na vprašanja uporabnikov. Prijave zlorab sprejemamo tudi prek prijavne točke na spletnem portalu, ob zaznanih grožnjah širših razsežnosti pa pripravimo obvestila za medije.**

VARNI NA INTERNETU
Od mene je odvisno vse.

OZAVEŠČANJE JAVNOSTI NA PODROČJU INFORMACIJSKE VARNOSTI

Ozaveščanje javnosti na področju informacijske varnosti je opredeljeno v 5. točki drugega odstavka 28. člena Zakona o informacijski varnosti, SI-CERT pa naloge izpolnjuje v številnih aktivnostih programa Varni na internetu. Vse izpeljane aktivnosti so financirane s sredstvi Urada Vlade Republike Slovenije za informacijsko varnost (URSIV).

BREZPLAČNI SPLETNI TEČAJ
O INFORMACIJSKI VARNOSTI

V SI-CERT-u že leta opažamo in opozarjamo, da se napadalci usmerjajo na mala in srednja podjetja, ki po podatkih revije Forbes predstavljajo že skoraj 50 % vseh žrtev vdorov. Leta 2017 smo v kampanji ob Evropskem mesecu kibervarnosti »Najstrašnejša žival je … miš!« prvič postavili v ospredje nevarnosti, ki prežijo na manjša podjetja. Pri podjetjih ni bilo pretiranega zanimanja za izobraževanje zaposlenih in dvig kibernetske kulture, kar pa se zadnji dve leti intenzivno spreminja. Tako v medijih kot na strokovnih konferencah je vedno več govora o dodatnem vlaganju v kader, opremo, zunanje varnostne preglede. Še največ pa je govora o primerih, ko je že prišlo do vdora in so bile posledice za organizacijo izredno negativne – ne le v finančnem smislu.

Pandemija in množično delo na daljavo sta nam dala še dodaten razlog, da se lotimo za nas novega področja – **zasnovali smo brezplačni spletni tečaj o osnovah informacijske varnosti za zaposlene Varni v pisarni. V ospredje smo postavili zaposlene, ki niso zgolj zreducirani na najšibkejši člen, ampak izpostavljamo, da so pogosto spregledani, nimajo možnosti izobraževanj ali pa so ta neprilagojena njihovemu nivoju znanja.**

Spletni tečaj Varni v pisarni na zelo enostaven, razumljiv in vizualno privlačen način zaposlenim predstavi osnove informacijske varnosti. Spletni tečaj je brezplačen, poteka kadarkoli na zahtevo, traja 30 minut in je prilagojen različnim delovnim mestom v organizaciji. Tečaj je primarno namenjen manjšim podjetjem, kjer sami skrbijo za svoj IT-oddelek ali nimajo jasnega nadzora nad delom zunanjih IT-izvajalcev, zaposleni pa pri svojem delu uporabljajo različne e-bančne in

druge plačilne storitve, spletne trgovine in družbena omrežja. Učne teme so razdeljene na module in prilagojene različnim delovnim procesom, zato je tečaj primeren tudi za druge organizacije, kjer ni sistematičnega pristopa k izobraževanju o informacijski varnosti.

MODUL OSNOVE ZA VSE pojasni, kje se skrivajo nevarnosti, ko zaposleni uporabljamo osnovno delovno orodje – elektronsko pošto. Modul se osredotoča na odpiranje priponk, prepoznavanju phishing zlorab in varovanje gesel.

MODUL ZA RAČUNOVODJE je namenjen vsem, ki imajo v podjetju dostop do spletne oz. mobilne banke. Računovodstvo in tajništvo sta pogosto tarči kibernetskih napadov, saj imajo zaposleni dostop do bančnih računov – ti pa so glavni cilj napadalcev. Obenem imata oddelka stik z vodstvom in drugimi zaposlenimi, tajništvo pa je običajno najpomembnejša vstopna točka za stranke in druge obiskovalce.

MODUL ZA MARKETING, PRODAJO, LOGISTIKO je namenjen zaposlenim, ki vsakodnevno veliko komunicirajo z zunanjimi partnerji, upravljajo kanale na družbenih omrežjih, naročajo blago v spletnih trgovinah, iščejo ugodne ponudbe.

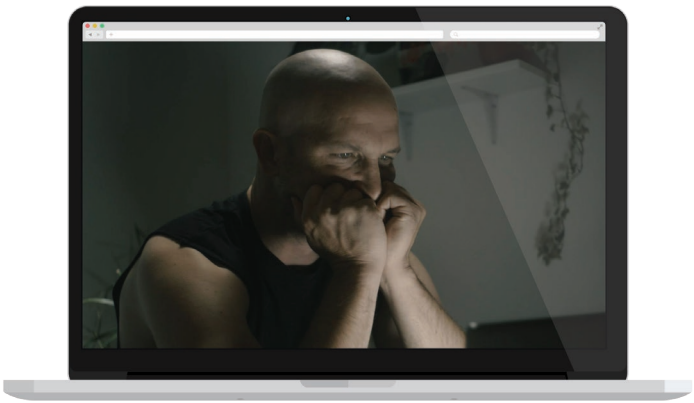
MODUL ZA IT je namenjen informatikom v podjetju in zunanjim vzdrževalcem. Zaposleni, ki skrbijo za varnost, morajo biti vedno na tekočem z najnovejšim dogajanjem, saj ravno oni predstavljajo prvi ščit med napadalci in podjetjem. Četudi gre za izkušene strokovnjake, lahko ob obilici različnih nalog mimogrede pozabijo na malenkost, ki ima lahko katastrofalne posledice.

Vsak modul je razdeljen na kratka poglavja. Tečajniki si najprej ogledajo uvod v temo, sledijo problematike in podajanje rešitev, na koncu pa rešijo kviz, ki jim omogoča pridobitev certifikata o opravljenem tečaju. Pri vsakem modulu so na voljo tudi dodatni izobraževalni materiali. **Tečaj je prosto dostopen na naslovu www.varnivpisarni.si**

VIDEO SERIJA KLIK –
ČLOVEŠKI OBRAZ SPLETNIH PREVAR

Spletna video serija zajema štiri dele, pri čemer v vsaki epizodi nastopajo nove osebe. V vsaki epizodi je predstavljena ena od najpogostejših spletnih prevar. V epizodi »Posel kariere« predstavimo malo podjetje, ki je postalo žrtev vrivanja v poslovno komunikacijo; »Kriptomanija« sledi zgodbi enega številnih uporabnikov, ki so nasedli investicijski prevari; video »Kdo je jaz?« združuje več spletnih prevar, ki jim je skupna kraja identitete, zadnja epizoda »Za ljubezen« pa je posvečena ljubezenskim prevaram. Skupno si je na kanalih Varni na internetu prek Facebooka in YouTuba serijo KLIK do zdaj ogledalo več kot 324 tisoč spletnih uporabnikov, pri čemer je najbolj priljubljena epizoda »Posel kariere« z malo več kot 137 tisoč ogledi.

Kadar je govora o spletnih prevarah, je v ospredju običajno statistika: število kibernetskih napadov, zneski oškodovanj, trendi naraščanja … Podatki brez imena ali obraza. Posledično spletne prevare in kibernetski vdori postanejo nekaj abstraktnega, nekaj, kar se nam nikoli ne more zgoditi. Resnica je seveda, da se za statistiko skrivajo ljudje, katerih zgodbe lahko imajo srečen ali pa malo manj srečen konec. V seriji z naslovom »KLIK« smo v SI-CERT-u izpostavili človeški vidik spletnih prevar, da bi področje kibernetske varnosti tako še bolj približali ljudem.



EVROPSKI MESEC KIBERNETSKE VARNOSTI – POMISLI, PREDEN KLIKNEŠ!

Evropski mesec kibervarnosti (ang. European Cyber Security Month) je vseevropska kampanja ozaveščanja, ki jo s podporo držav članic organizirata Agencija Evropske unije za kibernetsko varnost (ENISA) in Evropska komisija. Kampanja vsako leto poteka v oktobru, in sicer tokrat že drugič zapored pod sloganom »Premisli, preden klikneš« (ang. Think Before U Click).

Ves oktober je po Evropi potekalo na stotine dejavnosti, da bi z izobraževanjem in izmenjavo dobrih praks povečali ozaveščenost o kibernetski varnosti. Namen vseevropske pobude je obravnavanje varnostnih vprašanj v zvezi z digitalizacijo vsakdanjega življenja, ki so se ob pandemiji covida-19 dodatno namnožila. Zdaj je bolj kot kadar koli prej pomembno, da se uporabniki izobrazijo o digitalni varnosti, ker bodo le tako prepoznali tveganja in se učinkovito odzvali na kibernetske grožnje. Kampanja 2021 »Premisli, preden klikneš«, ki ljudi spodbuja k skrbnemu premisleku, predstavlja dva vidika kibernetske varnosti – **kibernetsko varnost doma in ukrepe, če pride do kibernetskega incidenta**.

Za ozaveščanje je ENISA pripravila vrsto izobraževalnih materialov v obliki kratkih videov in infografik, ki smo jih države članice delile na svojih kanalih. V videih so resnični posamezniki delili svojo zgodbo, kako so postali žrtev spletnih napadalcev ter predstavili korake za prepoznavanje omenjenih prevar in zaščito pred njimi. Infografike, ki so bile tematsko razdeljene v dva sklopa, so vsebovale glavne napotke za izboljšanje kibernetske varnosti doma in ukrepe ob kibernetskem incidentu.

SI-CERT je kot koordinator za Slovenijo že deveto leto zapored sodeloval v vseevropski pobudi z nacionalnim programom ozaveščanja Varni na internetu.

EVROPSKI
MESEC
KIBERNETSKE
VARNOSTI

Ključni nasveti za varnost vaših računov

Enako kot zaklepanje vhodnih vrat pred vlomilci, igra zaščita naših spletnih računov osrednjo vlogo pri obrambi pred spletnimi kriminalci - in gesla so ključnega pomena. Preverite nekaj nasvetov za varnost vaših spletnih računov.

1. Izberite močna gesla

Močnejše je vaše geslo, težje je vdreti v vaš račun.

Ustvarite gesla, ki so dolga najmanj 15 znakov ter vključujejo kombinacijo velikih in malih črk, številk in simbolov, če so dovoljeni.

To lahko uspešno storite z večbesednim geslom – uporabite stavek z neobičajnimi besedami ali besedami iz različnih jezikov.

Poleg tega za vse svoje spletne račune vedno uporabite enkratna gesla.

2. Uporabljajte upravitelja gesel

Upravitelj gesel je dober način, kako lahko poskrbite za svoja gesla.

Več zelo dobrih upraviteljev gesel je brezplačnih in enostavnih za uporabo. Z njimi boste ustvarili močna gesla in jih obvarovali.

Če ne želite uporabiti upravitelja gesel, si jih zapišite v beležnico ter jih shranite na varnem mestu stran od svojega računalnika.

3. Omogočite večfaktorsko avtentikacijo

Večfaktorska avtentikacija (npr. 2FA) omogoča dodatno raven varnosti za zaščito vaših računov.

Gre za metodo elektronske avtentikacije, pri kateri morate predložiti dve ali več dokazil („faktorjev") za potrditev svoje identitete in dostop do računa, na primer geslo in kodo, ki jo prejmete na svoj mobilni telefon. Dostop do vašega računa ni mogoč brez vnosa te kode.

4. Upoštevajte vse zgoraj navedeno!

Za dodatno varnost uporabite upravitelja gesel, s katerim boste ustvarili močna gesla in omogočite večfaktorsko avtentikacijo, kjer je mogoče ter tako kar najbolje obvarujte svoje račune.

enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

#CyberSecMonth

#ThinkB4UClick

Naslov publikacije: Poročilo o kibernetski varnosti za leto 2021

Avtor publikacije: Nacionalni odzivni center za kibernetsko varnost SI-CERT

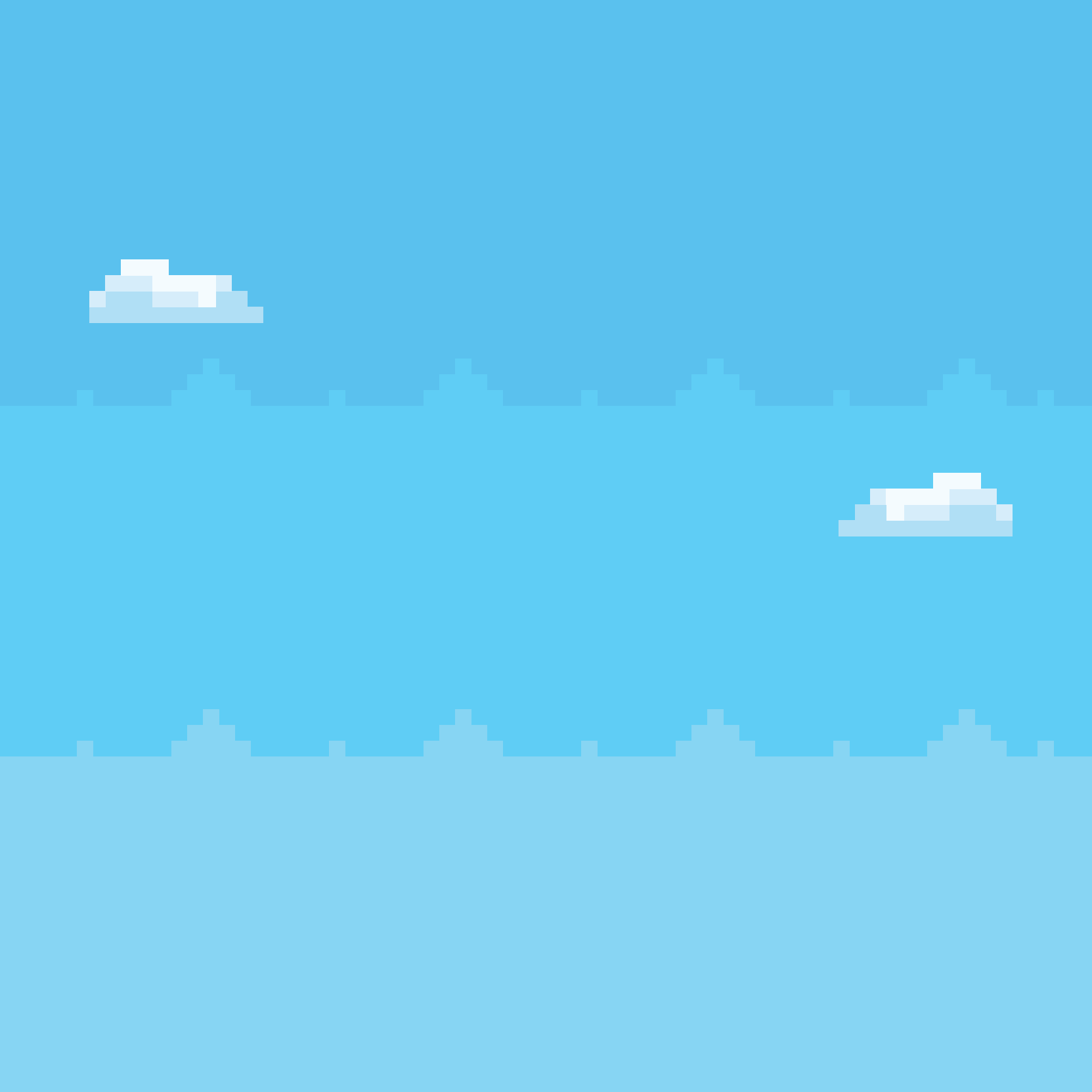
Leto izida: 2022

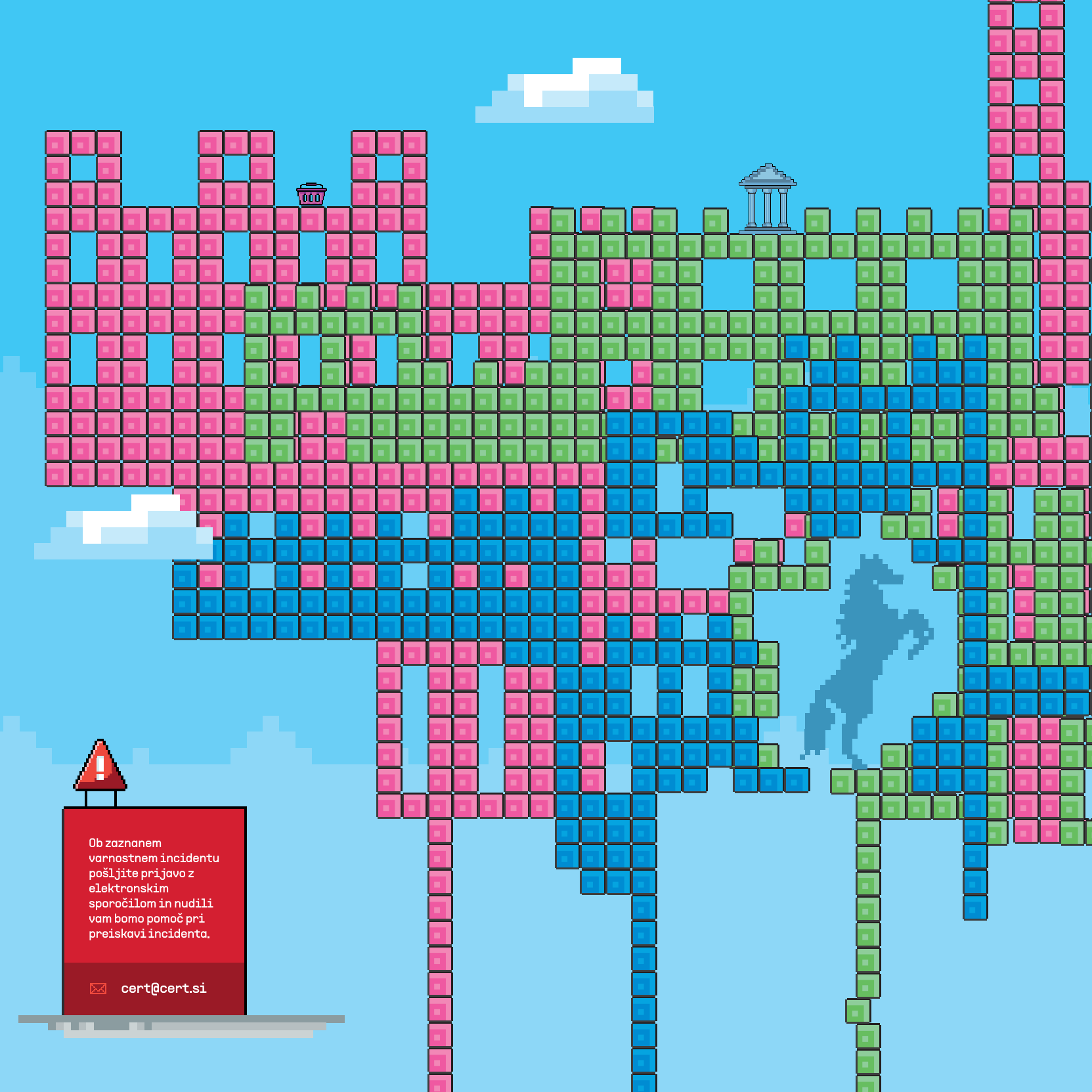
Naklada: 500 izvodov

Založnik: Akademska in raziskovalna mreža Slovenije

Oblikovanje in prelom: KOFEIN dizajn

Vsa letna poročila o omrežni varnosti v Sloveniji, ki jih izdajamo pri SI-CERT, so dostopna na naslovu www.cert.si/letna_porocila/.




Ob zaznanem varnostnem incidentu pošljite prijavo z elektronskim sporočilom in nudili vam bomo pomoč pri preiskavi incidenta.
cert@cert.si