POROČILO O KIBERNETSKI VARNOSTI 2024

Nacionalni odzivni center
za kibernetsko varnost
SI-CERT

si·cert
Nacionalni odzivni center
za kibernetsko varnost

SI-CERT

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

@SI-CERT, Slovenian National Computer Emergency Response Team
facebook.com/sicert
@sicert

Ozaveščanje javnosti na področju kibernetske varnosti
www.varninainternetu.si

facebook.com/varninainternetu
@varninanetu
instagram.com/varninainternetu

Vse dejavnosti odzivnega centra SI-CERT financira Urad Vlade Republike Slovenije za informacijsko varnost.

URSIV

KAZALO

UVODNIK

TRIDESET LET KIBERNETSKE VARNOSTI

Jeseni leta 1995 smo na SI-CERT-u iz švedskega kraljevega inštituta za tehnologijo KTH prejeli prvo prijavo incidenta, kar štejemo za začetek svojega delovanja. Namen odzivnih centrov za kibernetsko varnost je oblikovanje zavedanja o trenutnem stanju in vzdrževanje strokovnega znanja na področjih digitalne forenzike, analize zlonamerne kode ter postopkov odzivanja na kibernetske grožnje in incidente. Lahko bi rekel, da je to veljalo tako takrat kot tudi danes. Seveda pa se je v treh desetletjih marsikaj spremenilo. Digitalizacija je prežela naša življenja in temu primerno so posledice kibernetskega incidenta lahko danes veliko resnejše kot v časih modemov in IRC-a. Vendar smo v tem okolju tudi mi rasli in se strokovno krepili, zato lahko danes primerno obvladujemo sodobne kibernetske grožnje. Hitro se moramo prilagajati rasti incidentov ter novim uredbam in direktivam, ki kar po tekočem traku prihajajo iz Bruslja, a res je, da večinoma naslavljajo težave, ki jih moramo začeti reševati. SI-CERT je izvrstno vpet v mednarodno skupnost in dobro prepoznan v strokovni javnosti doma. Naš program Varni na internetu je velikokrat vzor drugim v Evropski uniji kot učinkovito in usmerjeno ozaveščanje na področju varne uporabe interneta. Glede tega smo tako jaz kot tudi moji sodelavci na SI-CERT-u z doseženim lahko zadovoljni.

Kaj pa bi izpostavili, da je zaznamovalo leto 2024? Izbrali smo tri teme. **Mobilne naprave in vsesplošna digitalizacija naših življenj** nas izpostavljajo ranljivostim naprav in včasih slabo zasnovanim aplikacijam, ki vsebujejo ranljivosti, te pa se lahko končajo slabo za posameznika ali podjetje. Tako rekoč vsakodnevno se ukvarjamo s **krhkostjo naše digitalne infrastrukture**, saj je bila (spet) digitalizacija tako hitra, da je veliko lukenj nezakrpanih. Razvoj platform družbenih omrežij nas je popeljal v **novo dobo družbenega inženiringa**, kjer ne le, da nas goljufi skušajo oropati, ampak so pod vprašajem tudi širši družbeni vidiki, kot je vplivanje na javno mnenje in izide volitev.

Izzivov nam ne bo zmanjkalo. Po kratkem pogledu nazaj se zato usmerimo naprej.

Gorazd Božič
Vodja SI-CERT

KLJUČNE ŠTEVILKE 2024

4.587
incidentov, od tega

790
tehnično zahtevnejših

1.583
primerov zvabljanja na lažna spletna mesta (phishing)

97
investicijskih prevar s kriptovalutami

163
novinarskih vprašanj

60
strokovnih predavanj in sodelovanj na okroglih mizah

3.421
novih tečajnikov na platformi Varni v pisarni

si·cert
Nacionalni odzivni center za kibernetsko varnost

2024 NA DLANI

JAN

Na forumu na temnem spletu neznanec v odkup ponudi podatke o klicih na številko 112, v katerih so tudi zdravstveni podatki kličočih. V javnosti se takoj začnejo širiti nepreverjene informacije o vzrokih, od vdora v lokalno gasilsko društvo, do kraje s strani zaposlenega.

FEB

Preiskujemo bančne trojance za mobilne naprave iz družine Anatsa, ki so bili uporabljeni pri finančnem oškodovanju več žrtev iz celotne države. Gre za prvi tovrstni primer zlonamerne kode za mobilne naprave, ki je ciljala tudi na uporabnike slovenskih bank.

MAR

Prejmemo prvo prijavo napredne oblike direktorske prevare, ciljane na slovensko podjetje. Prevara vključuje telefonski klic iz potvorjene telefonske številke direktorja, glas pa je ustvarjen s pomočjo t. i. deepfake tehnologije.

APR

Proruske hektivistične skupine izvedejo več napadov onemogočanja različnih spletnih mest organov državne uprave, podjetij in posameznikov. Glavni cilj napadov je širjenje strahu med prebivalci, medtem ko ne povzročijo veliko škode.

MAJ

Europol izvede operacijo Endgame, ki je onesposobila večje število botnetov (omrežje okuženih računalnikov). Na SI-CERT-u v nadaljevanju leta prejmemo podatke o okuženih računalnikih slovenskih uporabnikov, ki jih o okužbah obveščamo preko telekomunikacijskih operaterjev.

JUN

Dobivamo prve prijave uporabnikov o neobičajnih registracijah Telegram računov z njihovimi telefonskimi številkami. V nadaljevanju leta sledi še mnogo več prijav. Kot najverjetnejši razlog se kaže zloraba enega od sistemov za posredovanje SMS-sporočil.

JUL

Programska napaka pri posodobitvi varnostne aplikacije podjetja CrowdStrike povzroči globalne izpade več milijonov računalnikov. Napaka je ustavila letalski promet, bančne storitve, bolnišnice in drugo infrastrukturo, po grobi oceni pa je na globalni ravni povzročila več kot 10 milijard evrov škode.

AVG

Napadalci začnejo z izvajanjem naprednih phishing napadov na podjetja, ki poleg lažnega sporočila vsebujejo tudi element telefonskega klica, v katerem se predstavijo kot uslužbenci banke. Napadi povzročijo visoka finančna oškodovanja.

SEP

Pojavijo se informacije o zelo obsežnem vdoru v večje število telekomunikacijskih operaterjev v ZDA. Izkaže se, da gre za več let trajajočo vohunsko kampanjo, za katero stoji državno podprta APT skupina Salt Typhoon.

OKT

Univerza v Mariboru doživi kibernetski napad z izsiljevalsko programsko opremo, ki za dalj časa onesposobi njihovo infrastrukturo. Univerza takoj začne odpravljati posledice, kar v celoti traja več mesecev.

NOV

Agencija EU za kibernetsko varnost ENISA v Ljubljani v partnerstvu s SI-CERT-om organizira prvo mednarodno konferenco o ozaveščanju o kibernetski varnosti, ki je v celoti posvečena človeškemu dejavniku in spreminjanju vzorcev obnašanja na spletu.

DEC

V programu ozaveščanja Varni na internetu leto zaključujemo s pozivom k medgeneracijskemu sodelovanju. Pripravimo brezplačno zgibanko za manj vešče uporabnike z najpomembnejšimi pravili spletne varnosti.

PREDSTAVITEV ODZIVNEGA CENTRA SI-CERT

Nacionalni odzivni center za kibernetsko varnost SI-CERT je odzivni center za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij. Ustanovljen je bil leta 1995 in deluje pod okriljem pod okriljem Akademske in raziskovalne mreže Slovenije. Njegove primarne naloge so strokovna pomoč pri preiskovanju pri preiskovanju kibernetskih 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.

S sprejetjem Zakona o informacijski varnosti (ZInfV) leta 2018 je SI-CERT prepoznan kot nacionalna skupina CSIRT, katere naloge so opredeljene v 28. členu ZInfV **(op. v času izdaje publikacije je v veljavo stopil nov zakon ZInfV-1, ki ureja področje informacijske in kibernetske varnosti, vendar se letno poročilo v celoti nanaša na ZInfV)**. Kot ključne naloge v vlogi nacionalne skupine CSIRT izpostavljamo sprejem incidentov, ki jih priglasijo zavezanci, in ponujanje metodološke pomoči pri obvladovanju incidentov, saj pravilno in pravočasno odzivanje na kibernetske incidente bistveno prispeva k zagotavljanju visoke stopnje kibernetske varnosti v državi.

V vlogi zavezancev, ki imajo dolžnost priglasitve kibernetskih incidentov nacionalni CSIRT skupini, so tri skupine subjektov:

1

Zavezanci po Zakonu o informacijski varnosti so tako izvajalci bistvenih storitev kot ponudniki digitalnih storitev, ki morajo nacionalnemu CSIRT-u brez nepotrebnega odlašanja priglasiti incidente s pomembnim negativnim vplivom na delovanje bistvenih storitev, ki jih zagotavljajo. Pri določitvi, ali bi incident imel pomemben negativen vpliv, se upoštevajo dejavniki, ki so navedeni v Uredbi o določitvi bistvenih storitev in podrobnejši metodologiji za določitev izvajalcev bistvenih storitev.

2

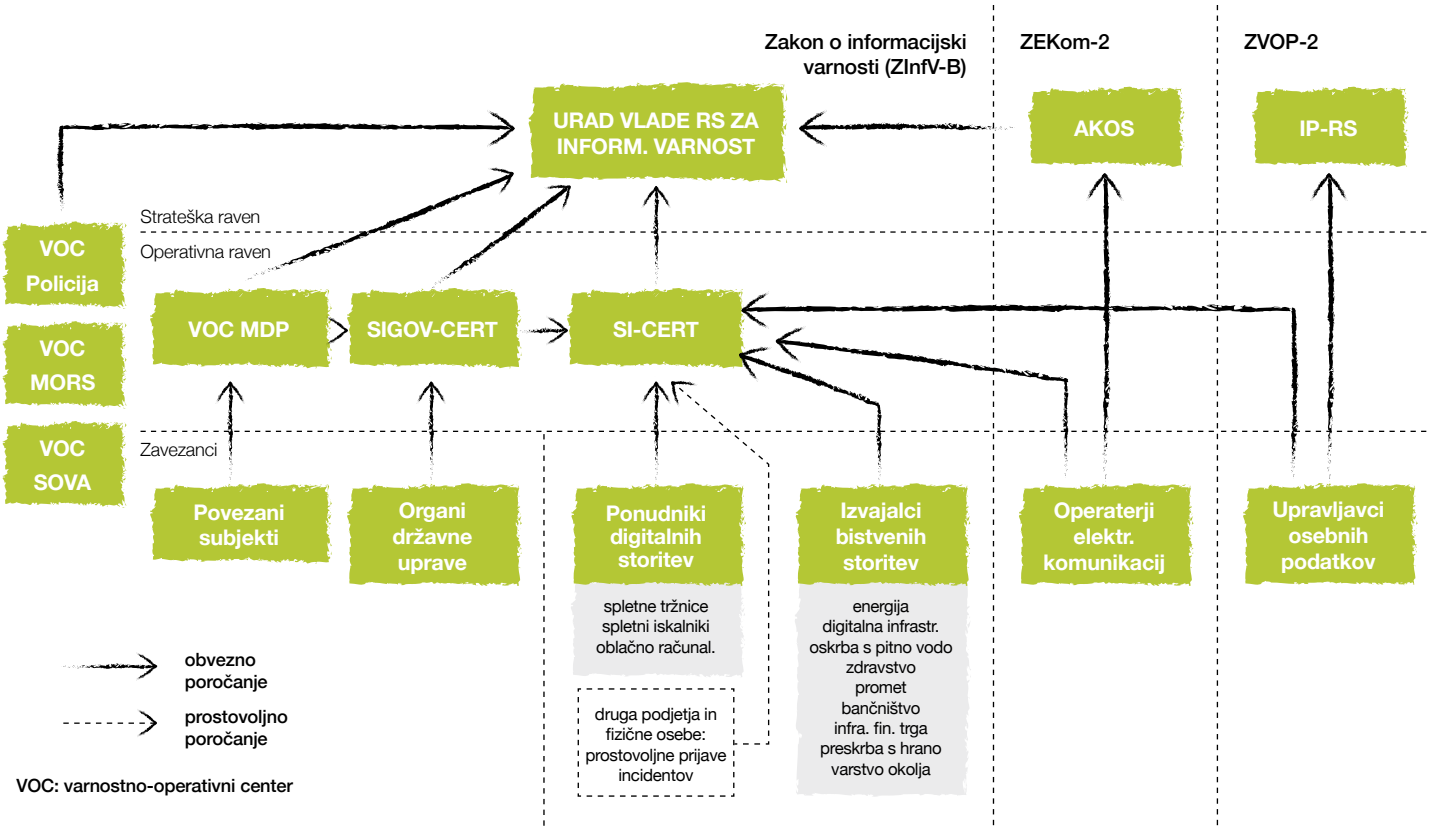
Zavezanci po Zakonu o elektronskih komunikacijah (ZEKom-2), ki je uveljavil Direktivo (EU) 2018/1972 o elektronskih komunikacijah. Zaradi večje učinkovitosti in takojšnjega razreševanja varnostnih incidentov morajo operaterji o varnostnem incidentu takoj obvestiti AKOS in SI-CERT (nacionalno skupino CSIRT).

3

Zavezanci po Zakonu o varstvu osebnih podatkov, ki je prenesel evropsko splošno uredbo o varstvu podatkov v slovensko zakonodajo in tudi ureja nacionalne posebnosti varstva osebnih podatkov. 23. člen ZVOP-2, kjer so opredeljene posebne obdelave osebnih podatkov, upravljavcem nalaga smiselno uporabo določbe o varnostnih zahtevah in priglasitvi incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na izvajalce bistvenih storitev, če upravljavcu glede teh obdelav ni treba izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

Dejavnosti centra SI-CERT v celoti financira Urad Vlade Republike Slovenije za informacijsko varnost, pristojni nacionalni organ za informacijsko varnost.

Storitve odzivnega centra SI-CERT so na voljo širši javnosti; po strokovno pomoč pri obravnavi kibernetskih incidentov se lahko obrnejo subjekti, ki jim to predpisuje zakon, prav tako tudi druge pravne in fizične osebe. Umeščenost centra SI-CERT v nacionalni okvir kibernetske varnosti in sistem odzivanja na incidente je razviden iz shematskega prikaza.



KDAJ PRIJAVITI INCIDENT?

Primer incidenta	Pričakovane dejavnosti centra SI-CERT
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 zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.
Opažen vdor v strežnik (razobličenje, zloraba podatkovnih zbirk, namestitev prikritih orodij storilca)	Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.
Phishing elektronska sporočila (potvorjena elektronska sporočila, ki vas napeljujejo, da geslo vpišete na lažni spletni strani)	Odstranjevanje in označevanje lažnih spletnih mest. Prepoznava širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.
Napad onemogočanja (poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja)	Ocena o uporabljenih sredstvih za napad, opredelitev mogočih 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 okužbe računalnika)	Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepih in možni identifikaciji storilca.

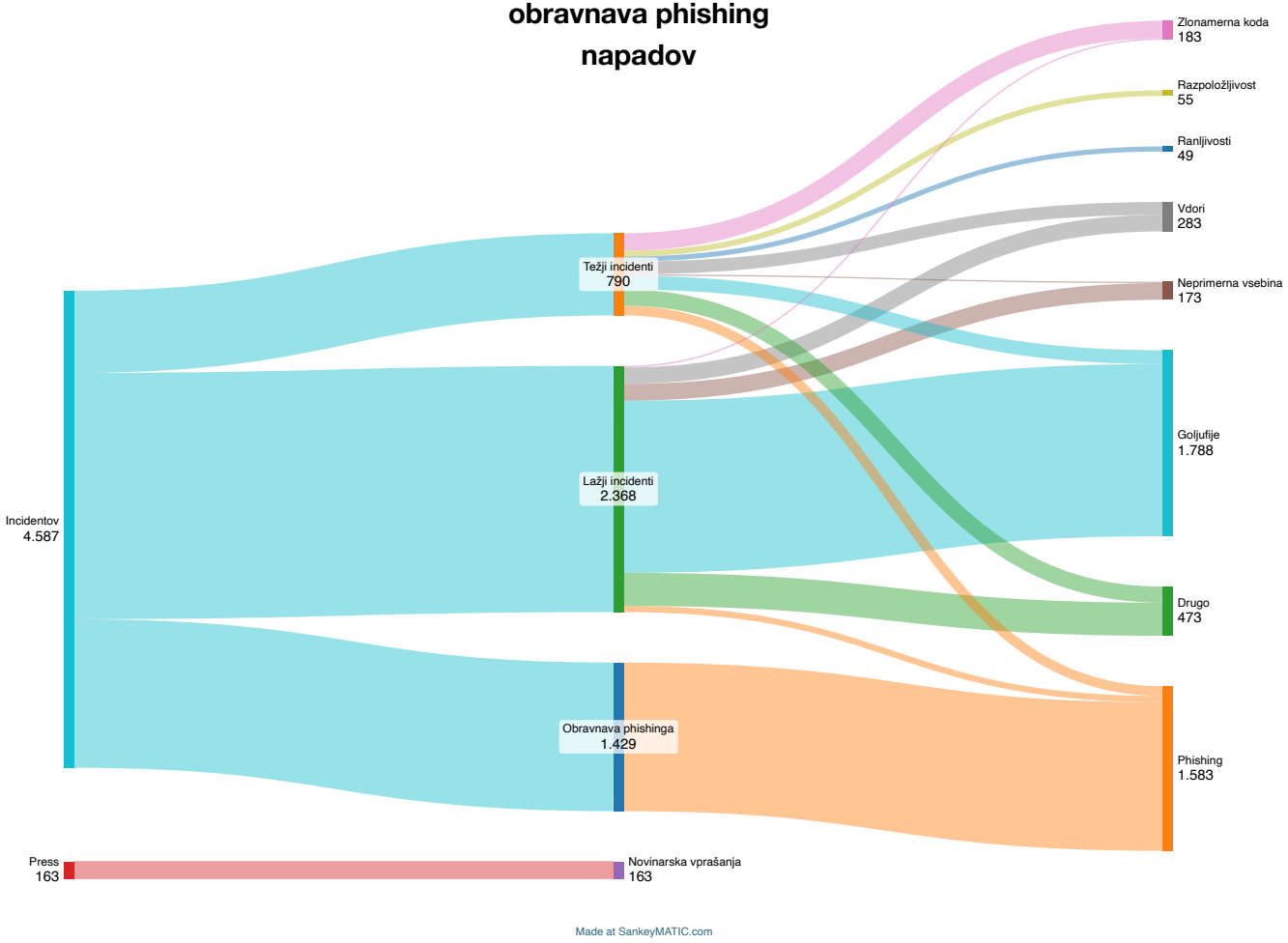
VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALNIKI

V letu 2024 smo 4.587 incidentov peljali skozi tri različne linije:

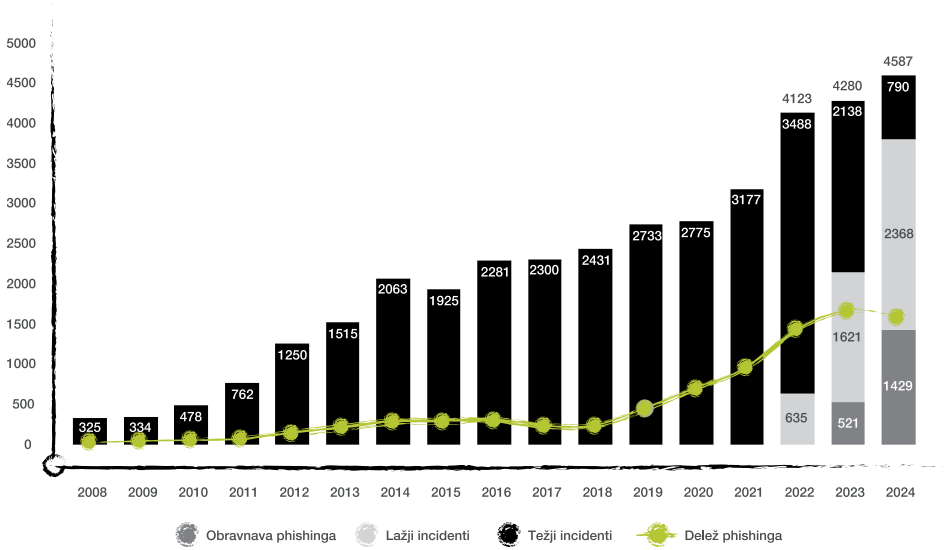
težji incidenti
(tehnično zahtevnejši)

lažji incidenti
(obravnava na prvolinijski podpori)

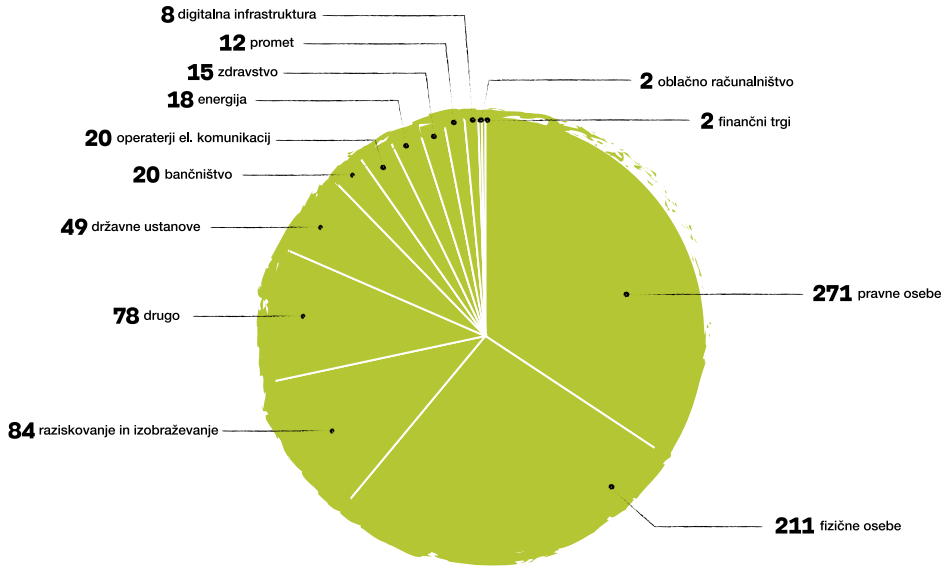
obravnava phishing napadov



INCIDENTI SKOZI LETA



PRIJAVITELJI PO SEKTORJIH



KLJUČNE BESEDE V OBRAVNAVANIH INCIDENTIH

VRSTE INCIDENTOV

Skupina	Vrsta incidenta	2021	2022	2023	2024
Neprimerna vsebina	Neželena sporočila	120	97	92	149
	Žaljiva vsebina	13	9	7	22
	Nasilna vsebina	0	1	0	2
Zlonamerna koda	Virus	29	8	9	13
	Črv	2	0	2	0
	Trojanski konj	171	278	140	110
	Vohunska programska oprema	2	2	1	0
	Dialler	0	0	1	0
	Rootkit	0	0	1	1
	Boti in botneti	9	8	4	8
	Nadzorni strežnik	0	1	0	0
	Izsiljevalski virus	64	45	32	25
	Orodje za oddaljen nadzor (RAT)	29	33	22	26
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	41	42	22	24
	Prestrezanje komunikacije	1	0	1	0
	Socialni inženiring	0	3	0	2
Poskusi vdora	Izkoriščanje znane ranljivosti	1	3	5	0
	Poskusi prijav, bruteforce in napadi s slovarjem	32	18	24	14
	Nova vrsta napada	0	0	0	0
Vdori	Zloraba priviligiranega uporabniškega računa	6	0	3	12
	Zloraba nepriviligiranega uporabniškega računa	105	112	150	212
	Napad na aplikacijo	5	6	11	19
Razpoložljivost	Napad onemogočanja	6	5	5	8
	Porazdeljen napad onemogočanja	27	17	21	55

	Sabotaža	0	0	1	**0**
	Izpad delovanja naprav ali omrežja	4	1	7	**6**
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	12	8	4	**14**
	Nepooblaščeno spreminjanje podatkov	22	15	18	**19**
	Odtekanje informacij	6	5	5	**5**
Goljufije	Nepooblaščeno izkoriščanje virov	5	6	13	**42**
	Intelektualna lastnina in avtorske pravice	10	12	2	**20**
	Kraja identitete	68	48	65	**64**
	Phishing sporočilo	765	1221	1610	**1539**
	Phishing spletno mesto	185	211	47	**44**
	Spletno nakupovanje	86	113	286	**239**
	Goljufija z vnaprejšnjim plačilom	182	181	177	**108**
	Izsiljevanje	138	346	329	**342**
	Druge goljufije	655	762	760	**973**
Ranljivosti	Odgovorno razkrivanje	12	4	9	**8**
	Razkritje ranljivosti	12	53	20	**18**
	Ranljivi sistemi in naprave	33	15	13	**23**
Drugo	Drugo	301	320	347	**418**
	Novinarsko vprašanje	9	1	0	**1**
Test	Namenjeno preizkusom	1	1	2	**2**
Skupaj		3169	4011	4268	**4587**
Nerazvrščenih		8	112	12	**0**
Vseh incidentov		3177	4123	4280	**4587**

— V tabeli Razvrstitev incidentov je razviden upad novinarskih vprašanj, ki pa je posledica tega, da smo v začetku 2021 spremenili njihovo obravnavo: uvedli smo naslov press@cert.si in ločeno linijo za odgovore. Skupaj smo v letu 2024 prejeli 163 novinarskih vprašanj.

VIŠINA OŠKODOVANJ V LETU 2024

Prijavitelji incidentov lahko ob podani prijavi na SI-CERT prostovoljno sporočijo tudi višino oškodovanja. Najvišji poskus oškodovanja je bil v višini **369.500 EUR** (kripto investicijska prevara), ki pa je bil na banki uspešno zaustavljen. Nekaj drugih izpostavljenih številk:

- povprečno oškodovanje pri nakupovanju na spletu: **1.300 EUR**;
- povprečno oškodovanje pri prevari z vnaprejšnjim plačilom (»nigerijska prevara«): **9.800 EUR**, najvišji posamični znesek: **40.000 EUR**;
- povprečno oškodovanje pri vrivanju v poslovno komunikacijo: **33.000 EUR**;
- najvišji poskus oškodovanja pri mobilnem bančništvu (transakcija zaustavljena pri banki): **200.000 EUR**.

Podatki slovenske policije za leto 2024

Vrsta goljufije	Število kaznivih dejanj	Škoda v EUR
investicijska vlaganja	705	19.516.000
vrivanje v poslovno komunikacijo in direktorske prevare	64	2.270.000
zlorabe elektronskega in mobilnega bančništva	90	2.742.000
ljubezenska prevara	46	574.000
nikoli dostavljen artikel	886	4.672.000
nigerijska prevara	16	260.000
lažni klici tehnične pomoči	16	150.000
sklenitev pogodbe	58	314.000
igra na srečo	4	7.500
lažni krediti	28	98.000
zloraba plačilne kartice	88	243.000

ODZIVNI ČAS PRI PRIJAVI INCIDENTA NA SI-CERT

odgovor poslan v
eni uri 27%

odgovor poslan v
dveh urah 41%

odgovor poslan v
12 urah 66%

odgovor poslan v
24 urah 87%

IZPOSTAVLJENE TEME V 2024

MOBILNE NAPRAVE IN DIGITALIZACIJA

Digitalizacija različnih vidikov naših življenj se je pospešila. Vse več storitev opravimo prek mobilnih in spletnih aplikacij, od naročanja k zdravniku, prevzemov paketov do bančnih opravil in naročanja hrane. To so hitro spoznali tudi spletni napadalci, ki so izkoristili »uporabniku prijazne« in včasih prehitro razvite aplikacije, ki so podlaga za nove poslovne modele. Končni uporabnik pa pogosto sam nosi odgovornost, čeprav je bil pravzaprav porinjen v omenjeni model in nima možnosti izbire. Smishing napadi v imenu bank in dostavnih podjetij, napredne zlonamerne mobilne aplikacije, kjer v primeru okužbe uporabnik ne more prepoznati in zaustaviti kraje denarja z računa, investicijske sheme v kriptovalute, ki so zgolj spletna fasada, ter neovirano oglaševanje goljufij na oglaševalskih platformah in družbenih omrežjih iz leta v leto povečujejo število prijavljenih incidentov in oškodovanj fizičnih oseb.

KRHKOST DIGITALNE INFRASTRUKTURE

Ne mine dan, da ne bi prepoznali novih ranljivosti. Morda se sliši pretirano, vendar je katalog znanih ranljivosti CVE (Common Vulnerabilities and Exposures) v letu 2024 dobil več kot **34.000 novih oznak za različne ranljivosti *naprav z digitalnimi komponentami*** (če si izposodimo terminologijo Akta o kibernetski odpornosti, ki želi tovrstne težave nasloviti). Med njimi so tudi *kritične ranljivosti* naprav, ki naj bi poskrbele za boljšo zaščito naših omrežij in storitev, kot so požarne pregrade, VPN naprave, platforme za množično upravljanje mobilnih naprav in še kaj. Posledice ranljivosti so lahko različne: od kraje podatkov, proženja izsiljevalskih virusov in resnih motenj poslovanja, uporabe zlorabljenih naprav s strani storilcev za zakritje sledov do izvajanja napadov onemogočanja. SI-CERT z obveščanjem skrbnikov prepoznanih ranljivih ali celo že zlorabljenih sistemov gasi požare, trendi pa zelo jasno kažejo, da bomo morali v bodoče krepiti kapacitete na tem področju in poskrbeti za res zelo hiter odziv, še posebej, ko gre za ranljivosti ničtega dne ali t. i. »0-day« ranljivosti, kjer uradni popravek še ni na voljo, napadalci pa jo že izkoriščajo.

DRUŽBENI INŽENIRING POVSOD OKOLI NAS

Družbeni inženiring (angl. social engineering) je v najbolj enostavni obliki manipulacija, s katero vas želi nekdo prepričati o nečem, kar ni resnično. Na primer to, da ste podedovali milijone od neznanega sorodnika v tujini ali pa, ko vam zaposleni sporoča, da je spremenil bančni račun. Vendar pa lahko vidimo, kako ta pojem z leti dobiva nove razsežnosti. Bodisi v napadih onemogočanja, ki želijo vnesti nemir in negotovost v družbo, s povzročanjem panike ob množičnih (na srečo lažnih) obvestilih o podtaknjenih bombah v šolah in vrtcih ali pa s financiranjem kampanj vplivnežev na družbenih omrežjih. Te lahko v nekaj tednih pripeljejo enega od kandidatov na predsedniških volitvah od neprepoznavnosti do skorajšnje zmage. S tega vidika bomo potrebovali resen razmislek v družbi in širši skupnosti o tem, kako takšne manipulacije sploh ukrotiti.

KLJUČNA OPAŽANJA V 2024

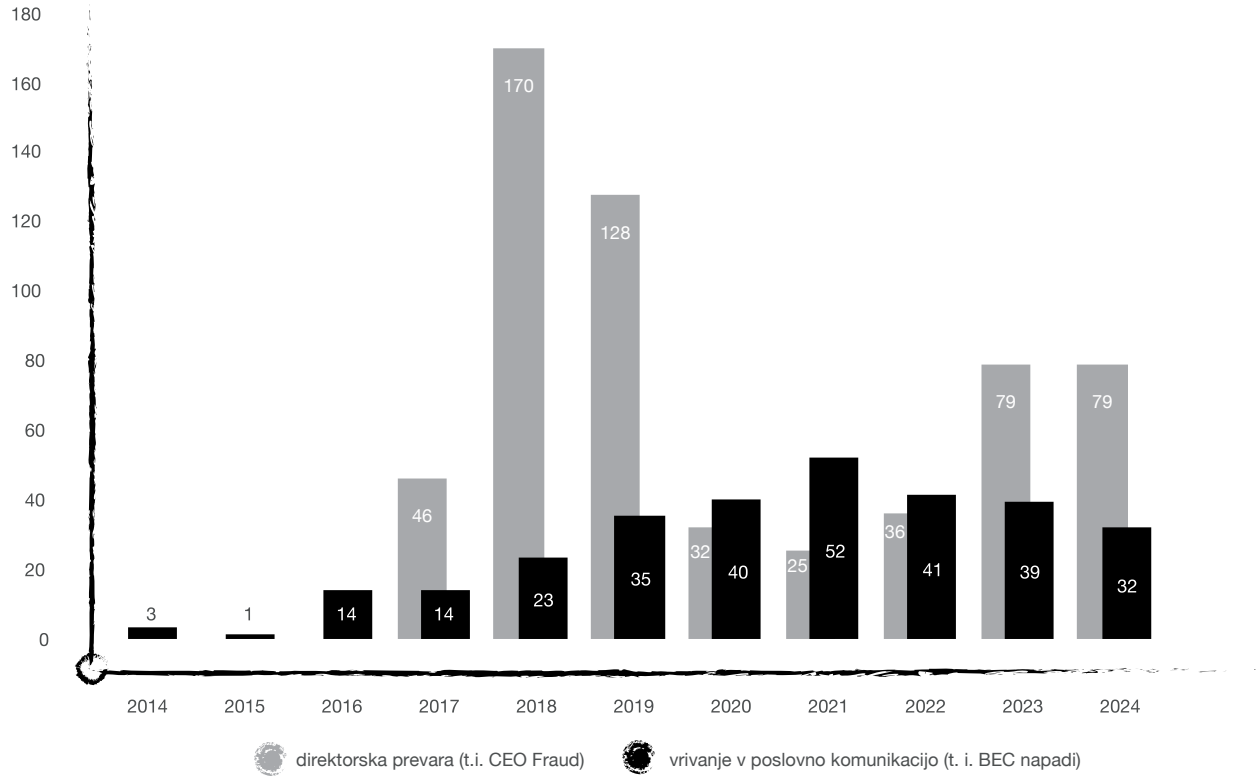
INDIVIDUALIZIRANI PHISHING NAPADI S HUDIMI POSLEDICAMI

Iz obravnavanih incidentov ugotavljamo, da je napredne phishing napade vse težje prepoznati. Napadalci v napadih družbenega inženiringa uporabljajo najrazličnejše trike, tako psihološke kot tehnološke. Opazna je vse pogostejša uporaba različnih orodij generativne umetne inteligence, zaradi česar je lažna sporočila čedalje težje ločiti od legitimnih. Zasledili smo napade, v katerih so napadalci s pomočjo t. i. deepfake posnetkov prevzeli identitete različnih oseb in na ta način poskušali vplivati na žrtve. Izpostavljamo tudi ciljane napade preko zasebnih stikov. Klasični napadi, pri katerih napadalci pošljejo množico sporočil in upajo, da bo majhen del uporabnikov nasedel, se čedalje bolj umikajo napadom, pri katerih napadalci ciljajo na točno določenega posameznika, s katerim vzpostavijo komunikacijo preko telefonskega klica ali zasebnega sporočila. Zaradi individualne obravnave je verjetnost, da žrtev ne bo prepoznala napada, zelo velika. Napadalci vzpostavijo stik z nami na način, za katerega marsikdo niti v sanjah ne bi pomislil, da bi lahko vodil k zlorabi, npr. kot kupec izdelka, ki ga prodajamo preko malega oglasa.

Napadalci lahko stik z žrtvijo vzpostavijo preko malega oglasa.

Primer takšnih napadov so tudi sofisticirani napadi vrivanja v poslovno komunikacijo (t. i. BEC napadi), pri katerih napadalci vdrejo v poštni sistem podjetja in v primeru zaznave pošiljanja fakture poslovnemu partnerju v sporočilu spremenijo podatek o bančnem računu. Po eni strani so tovrstni napadi tehnično dokaj enostavni, po drugi pa jih zaposleni zelo težko prepoznajo. Ker napadalcem omogočajo izredno velike zaslužke ob majhnem vložku, pričakujemo, da bodo ti napadi čedalje pogostejši ter s časom tudi čedalje bolj sofisticirani, zaradi česar jih bo vse težje prepoznati in preprečiti.

— V letu 2024 smo v javno objavljen seznam phishing strani dodali 1.430 phishing URL naslovov.



Lažna spletna stran ene od slovenskih bank. Po vpisu začetnih podatkov se pojavi obvestilo, da vas bodo poklicali iz banke.

— Povprečno oškodovanje pri vrivanju v poslovno komunikacijo (BEC prevara) v letu 2024: 33.092 €

V letu 2024 smo prvič zaznali primere naprednih phishing napadov na podjetja. Napad se kot običajno začne z lažnim elektronskim sporočilom banke, običajno pod krinko obvestila o posodobitvi digitalnega bančništva. Elektronska sporočila so razposlana na javno dostopne e-naslove podjetij.

Nato sledi telefonski klic, kjer se klicatelj predstavi kot bančni uslužbenec in ponudi, da pomaga pri postopku posodobitve. Pogovor v lepi slovenščini dodatno pripomore k verodostojnosti poslanega sporočila. Klici so opravljeni iz slovenskih telefonskih številk, ki pa so praviloma potvorjene (t. i. spoofing). Napadalci lahko ponaredijo celo telefonsko številko banke. Preko klica poskušajo izvabiti še dodatne avtentikacijske kode ali žrtev nagovoriti, da sama potrdi dostop. Tovrsten napad omogoči dostopi do bančnega računa podjetja in posledično visoko finančno oškodovanje.

ŽRTEV JE LAHKO VSAK

Vsesplošna digitalizacija naših življenj v zadnjih letih je prinesla nova tveganja. Na nekatera od njih se je zelo težko pripraviti, za nekatere uporabnike je to praktično nemogoče. Žrtev kibernetskega napada lahko postane čisto vsak posameznik ali organizacija. Če so napadalci včasih iskali enostavne tarče, ki zaradi minimalnih ali zastarelih varnostnih ukrepov dajejo »hitre rezultate«, so danes tarče tudi organizacije z visoko razvito varnostno kulturo in dosledno uporabo varnostnih ukrepov.

Končni rezultat kibernetskega napada na posameznike je največkrat kraja denarja, končni rezultat napada na organizacijo pa detonacija izsiljevalskega virusa (ransomware).

Primer povečanja prometa med volumetričnim DDoS napadom.

— Podobno kot pravimo, da je vsak posameznik lahko žrtev spletne goljufije, če goljuf le nastavi pravo vabo, je lahko tudi vsaka organizacija žrtev kibernetskega napada, če je le dovolj močan interes na strani napadalcev.

UČINKOVITI NAPADI SO LAHKO ZELO POCENI

Napadi onemogočanja (t. i. DDoS napadi) na številna spletna mesta slovenskih državnih institucij marca in aprila 2024 so pokazali, da napadalci ne potrebujejo strokovnega znanja ali lastne infrastrukture za izvedbo napadov, ki žrtvi povzročijo precej težav. Napadi onemogočanja so tehnično precej nezahtevni napadi in jih lahko za nekaj 10 evrov vsakdo naroči na spletu, pod črto pa povzročijo veliko hrupa z relativno malo vložka in se zato lahko konec koncev izkažejo kot učinkoviti. Ustrezna pripravljenost lahko pomaga.

MAJHNOST NI ZAŠČITA

Slovenija ni varna oaza, odmaknjena od sveta specializiranih bančnih trojancev za mobilne naprave. Aplikacije preko dodeljenih pravic storitev dostopnosti (ang. accessibility service) pridobijo vse potrebne podatke za odklep naprave, prijavo v mobilno banko in izvedbo nakazila denarja. Zlonamerne aplikacije so bile dostopne na tržnici aplikacij Google Play Store pod imeni »Phone Cleaner – File Explorer« in »PDF Reader: File Manager«. Pri vseh zabeleženih oškodovanjih je bilo preko mobilne banke opravljeno nakazilo finančnih sredstev oškodovancev na IBAN račune kripto menjalnice. Takšni napadi izpostavljajo temne plati pospešene digitalizacije naših življenj.

— Vrsto let so bile slovenske bančne mobilne aplikacije pod radarji napadalcev, februarja 2024 pa smo na SI-CERT-u prvič dobili v analizo zlonamerne aplikacije, t. i. banking trojan infostealer iz družine Anatsa, ki so bile uporabljene pri finančnem oškodovanju več slovenskih žrtev.

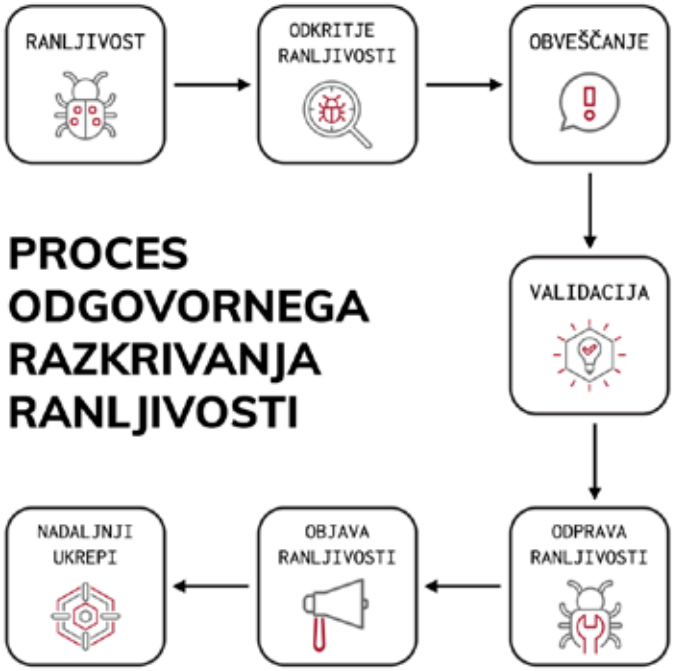
Shematski prikaz delovanja trojanskega konja Anatsa.

RANLJIVE NAPRAVE

Na spletu je še vedno preveč prosto dostopnih administrativnih vmesnikov različnih strežnikov in omrežnih naprav. Napadalci vseskozi skenirajo celoten splet z različnimi orodji za iskanje prosto dostopnih vmesnikov. Ti jim omogočajo, da hitro preiščejo velike segmente in identificirajo naprave, ki imajo dostopne administrativne vmesnike ali nameščene ranljive aplikacije in druge programske komponente. Sledijo nepooblaščen vstop v napravo in omrežje, izkoriščanje ranljivosti in nadaljnji napadi. Končni rezultat je lahko že omenjena detonacija izsiljevalskega virusa (ang. ransomware) ali vključitev zlorabljenih naprav v infrastrukturo napadalcev, s katero izvajajo nadaljnje napade.

SI-CERT na svoji spletni strani izdaja opozorila za upravitelje omrežij in širšo javnost o pomembnih ranljivostih in grožnjah v elektronskih omrežjih. Prav tako je vsako objavljeno varnostno obvestilo poslano naročnikom e-novičnika Odziv. Skrbnike ranljivih in izpostavljenih sistemov pogosto obveščamo tudi neposredno ali preko telekomunikacijskih operaterjev. Skrbniki bi morali poskrbeti, da so kontaktni naslovi domen in omrežij vedno aktualni.

— V primeru odkritja ali zaznave ranljivosti se lahko sproži postopek usklajenega razkrivanja ranljivosti, v katerem SI-CERT nastopa v vlogi koordinatorja.



PROCES ODGOVORNEGA RAZKRIVANJA RANLJIVOSTI

SPREGLEDAN ČLOVEŠKI DEJAVNIK

Močno zasidrano prepričanje, da je človek najšibkejši člen v verigi varnosti, se počasi spreminja. Tudi sami smo večkrat izrekli to trditev, vendar danes vidimo, da je človek oz. zaposleni pogosto zapostavljen člen, saj so največkrat zaposleni deležni osnovnega usposabljanja o kibernetski varnosti šele takrat, ko podjetje že doživi kibernetski incident. Pogosto je zaposleni glavni krivec za vse (ker je odprl zlonamerno priponko, ker je vnesel podatke na phishing strani ipd.) tudi takrat, ko bi organizacija lahko storila veliko več z vidika tehničnih in organizacijskih ukrepov. Če znajo zaposleni prepoznati lažno ali sumljivo sporočilo ter o tem tudi obvestijo ostale, lahko predstavljajo prvo linijo obrambe, potem ko zatajijo vse ostale tehnične zaščite. SI-CERT podjetjem in organizacijam nudi brezplačen spletni tečaj o informacijski varnosti za zaposlene, ki je na voljo na enaslovu www.varnivpisarni.si

— Skupno je od oktobra 2021 spletni tečaj Varni v pisarni opravilo že več kot 10.000 tečajnikov, od tega 3.421 v letu 2024.

NACIONALNI PROGRAM OZAVEŠČANJA O KIBERNETSKI VARNOSTI

ČLOVEK – EDEN OD STEBROV KIBERNETSKE VARNOSTI

V času pospešene digitalizacije je ključno zagotoviti varnost, saj je zaupanje v številne nove storitve in tehnologije prvi predpogoj, da uporabniki izkoristijo ves potencial, ki ga digitalizacija prinaša. Pomemben dejavnik, ki prispeva k zagotavljanju varnosti, pa je tudi opolnomočen uporabnik, ki se zaveda pomena varne in odgovorne rabe interneta, pomembnosti varovanja osebnih podatkov in zaščite naprav.
Posameznik je povsem enakovreden steber zagotavljanja informacijske varnosti, ki stoji ob boku tehnologijam in organizacijskim ukrepom. Statistike kažejo, da so še vedno najuspešnejši (in najcenejši) napadi, ki ciljajo na posameznika, saj so v samem vrhu napadi družbenega inženiringa. Gre za različne oblike spletnih goljufij in predvsem napadov z zvabljanjem (ang. phishing), ki so v zadnjih nekaj letih zabeležili globalen skok in so trenutno najpogostejša grožnja, ki preti povprečnemu spletnemu uporabniku. V večini primerov napadalci kot vstopno točko izberejo elektronsko pošto, v zadnjem času pa močno narašča tudi število napadov prek SMS-sporočil in aplikacij za hipno sporočanje.

— Gre za incidente, kjer napadalci izkoristijo človeške ranljivosti, podobno kot bi poiskali in izkoristili napako v programski kodi.

Zaupanje v programske rešitve nas pred takšnimi zlorabami ne bo vedno obvarovalo. Še vedno je glavna **rešitev izobraževanje spletnih uporabnikov**, in sicer ne zgolj s komunikacijskimi akcijami, ki naslavljajo posameznika v njegovem domačem okolju, ampak **tudi s kontinuiranim, hkratnim izobraževanjem v poslovnem okolju.** Na SI-CERT-u že leta opozarjamo, da je še vedno (pre)pogosto prepričanje, da manjša podjetja niso zanimiva za spletne napadalce, kar ne drži. Če zaposleni nimajo ustreznih znanj in veščin, da bi prepoznali nevarnost, so napadalci pogosto uspešni.

Obenem tudi nove spletne platforme prinašajo nove priložnosti za napadalce. Če je zadnjih deset let poglaviten motiv napadalcev ostal enak – prepričati uporabnike v nakazilo denarja, pa so se močno spremenile komunikacijske poti, po katerih pridejo do svojih žrtev**. Nove spletne storitve, nove oblike plačevanja na spletu, predvsem pa nove platforme družbenih omrežij so prinesle številne priložnosti za spletne napadalce.** Pomembno se je zavedati tudi, da kibernetska varnost ni neprijetna naloga enega oddelka znotraj podjetja ali ene organizacije v državi. Gre za skupno odgovornost vseh, saj se kibernetske grožnje ne ustavijo znotraj državnih meja.**Kibernetska varnost zadeva vse** – »Cyber Security Is Everyone's Business« – in iskanje učinkovitih odzivov nanje je eden ključnih globalnih izzivov našega časa.

PODATKI NA DLANI

Nacionalni program ozaveščanja Varni na internetu je še ena izmed zakonsko opredeljenih nalog, ki jih izvaja SI-CERT. Ozaveščanje javnosti na področju informacijske varnosti je opredeljeno v 5. točki drugega odstavka 28. člena Zakona o informacijski varnosti, SI-CERT pa naloge izpolnjuje s številnimi dejavnostmi programa Varni na internetu.

Cilji

Kot glavni cilj opredeljujemo **opolnomočenje spletnih uporabnikov, da bodo znali prepoznati različna spletna tveganja in nevarnosti ter ustrezno zaščititi svoje naprave in uporabniške račune**. Prvi pogoj pa je, da uporabniki razumejo vrednost podatkov, ki jih varujejo – ne le finančnih (podatki kreditne kartice, finančna sredstva) in poslovnih, ampak tudi svoje zasebnosti.

Problematike

Program pokriva ključne problematike: okužbe z zlonamerno kodo, vdore v uporabniške račune, lažne spletne trgovine, različne oblike spletnih goljufij, phishing kraje podatkov.

Koga nagovarjamo?

- ODRASLI UPORABNIKI: Nagovarjamo **uporabnike, starejše od 25 let**, saj ta populacija že uporablja storitve spletnega bančništva in tudi opravi največji delež spletnih nakupov. Poleg njih pa so **najranljivejši uporabniki na spletu pripadniki starejše generacije**. To so večinoma upokojenci in delovno neaktivni prebivalci, ki niso več vpeti v formalne procese izobraževanja, hkrati pa niso deležni dodatnih izobraževanj o kibernetski varnosti.
- ZAPOSLENI, SAMOZAPOSLENI, MANJŠA PODJETJA: Druga ciljna skupina so **zaposleni v manjših podj**etjih, vodstva manjših podjetij in IT-kader, saj potrebujejo bolj specifične napotke in priporočila, hkrati pa imajo omejene vire.

Z več kot 500 objavljenimi članki smo v Sloveniji nedvomno referenčna točka, ko govorimo o kibernetski varnosti v najširšem smislu. V letu 2024 smo dodali 12 novih opozoril in priporočil v obliki člankov na spletni strani www.varninainternetu.si. Poslali smo tudi 22 edicij novičnika Varne novice, v katerem dvakrat mesečno izpostavimo aktualne prevare in nasvete za zaščito. **Novičnik zato dosega nadpovprečno visoko stopnjo odpiranja – povprečno je novičnik odprlo 50 % naročnikov, ki jih je bilo do konca leta že 12.038.**

Primer elektronskega novičnika Varne novice

KAKO GRADIMO SKUPNOST NA DRUŽBENIH OMREŽJIH?

Preko kanalov družbenih omrežij vsakodnevno komuniciramo z uporabniki. Ti na eni strani redno delijo naša opozorila o spletnih prevarah, na drugi pa se na nas obrnejo, ko sami zasledijo nekaj sumljivega. Na prejete primere prevar se odzovemo v najkrajšem možnem času in pripravimo objave in opozorila za svoje kanale. Na ta način gradimo trdno skupnost na področju kibernetske varnosti ter lažje širimo znanje in zavedanje o kibernetskih grožnjah med čim širši krog uporabnikov. Do konca leta smo z več kot 250 objavami na Facebooku, 104 na Instagramu in več kot 500 »storyji« zgradili bazo 43.819 sledilcev na Facebooku ter več kot 3.900 sledilcev na Instagramu.

— Hkrati se na družbenih omrežjih, s katerimi upravlja Meta, srečujemo tudi z omejitvami, ki nam otežujejo informiranje uporabnikov, saj naše vsebine (čeprav informativne in ozaveščevalne narave) algoritem pogosto prepozna kot kršitev standardov skupnosti, ki jih določa podjetje Meta.

Posledično pride do onemogočanja oglaševalskega računa, pa tudi naše organske objave so pod drobnogledom. **Na predstavništvo Mete na Poljskem smo naslovili več dopisov, vendar nismo prejeli odgovora.**

Ob tem opažamo še paradoks: medtem ko mi uporabnike opozarjamo na prevare, napadalci isto platformo nemoteno izrabljajo za oglaševanje in zvabljanje uporabnikov neposredno v spletne prevare, česar pa Meta ne prepozna kot spornega. To frustrira tudi naše sledilce, ki v komentarjih in sporočilih pogosto opozarjajo, da Meta nezakonitih vsebin, kljub več prijavam, ne odstrani.

KAJ ZANIMA UPORABNIKE?

Trendi na družbenih omrežjih se vse bolj nagibajo v smer kratkih, dinamičnih in zabavnih video vsebin. Kljub temu pa uporabniki še vedno cenijo ažurnost in uporabnost naših vsebin. Ker imamo neposreden vpogled v dogajanje in statistiko na področju spletnih prevar, lahko opozorila in nasvete za zaščito pripravljamo sproti – v skladu z aktualnimi spletnimi grožnjami.

Odličen odziv praviloma dosegajo prav objave, v katerih obravnavamo primere spletnih prevar, na katere nas opozorijo uporabniki. Tako smo lahko še bolj relevantni, odzivni in uporabnikom bližje.

Največ zanimanja običajno spodbudijo opozorila in videi o kripto investicijskih prevarah.

— Ob vsem tem pa hkrati opažamo izrazit kontrast med dejanskim stanjem – torej naraščajočim številom spletnih prevar in finančno škodo, ki jo te povzročajo, ter dojemanjem spletnih prevar v javnosti. Mnogi jih še vedno vidijo kot nekaj obrobnega ali banalnega, kar se »zgodi drugim«, predvsem manj digitalno pismenim ali starejšim.

EVROPSKI MESEC KIBERNETSKE VARNOSTI

OB EVROPSKEM MESECU KIBERNETSKE VARNOSTI SMO OPOZORILI NA PORAST LAŽNIH SMS-SPOROČIL

Vsako leto oktobra obeležimo Evropski mesec kibervarnosti, katerega cilj je povečati kibernetsko varnost in ozaveščenost. V tokratni kampanji smo izpostavili porast smishing prevar – zavajajočih SMS-sporočil in sporočil prek aplikacij (npr. Viber,

WhatsApp), s katerimi napadalci poskušajo pridobiti finančne podatke. V letu 2023 je bilo zabeleženih 216 primerov smishing napadov, kar je skoraj petkrat več kot leta 2022.

— Policija je v povezavi s phishingom in smishingom leta 2023 zabeležila kar 3,5 milijona evrov škode.

Uporabnike smo, poleg oglasov na družbenih omrežjih, naslavljali tudi prek TV ekranov. **Z realiziranimi 1.919 objavami na TV postajah z nacionalnim dosegom smo v 83 % dosegli populacijo, starejšo od 45 let.**

S kampanjo smo želeli dvigniti raven ozaveščenosti o najpogostejših prevarah, ki ciljajo na uporabnike pametnih telefonov. Z animiranimi video vsebinami smo predstavili manipulativne taktike napadalcev, zaradi katerih so tovrstni napadi uspešni. To so predvsem ustrahovanje (»ukrepajte takoj«, »vaš račun bo izbrisan« ipd.), prenasičenost z informacijami in trenutki nepozornosti.

S komunikacijsko kampanjo smo nato nadaljevali še v mesecu novembru, ki zaradi črnega petka in drugih dni, povezanih z nakupovanjem pred decembrskimi prazniki, ponuja idealen poligon spletnim napadalcem, ki z lažnimi sporočili v imenu bank in dostavnih služb ciljajo na pridobivanje podatkov kreditnih kartic uporabnikov.

TV-oglasa, predvajana v času meseca kibervarnosti.

Dejavnosti na družbenih omrežjih

Kampanja ozaveščanja v okviru meseca kibervarnosti je potekala tudi na družbenih omrežjih Facebook in Instagram. Doseg celotne kampanje je bil 178.390 uporabnikov v ciljni skupini 45+. Oglasi so uporabnike vodili na prispevek na spletni strani Varni na internetu, kjer so lahko prebrali podrobnejšo razlago anatomije tovrstnih lažnih sporočil. Ključno sporočilo kampanje je bilo, da spletni napadalci pogosto izkoriščajo strah – zato naj bodo uporabniki previdni pri klikanju na povezave v SMS-sporočilih in naj ne nasedajo grožnjam o blokadi računa, zavrnjenih pošiljkah ali plačilu carinskih stroškov.

PRVA MEDNARODNA KONFERENCA O OZAVEŠČANJU V KIBERNETSKI VARNOSTI

Agencija EU za kibernetsko varnost ENISA je v partnerstvu s SI-CERT-om organizirala prvo mednarodno konferenco o ozaveščanju o kibernetski varnosti pod geslom **»Novi pristopi k ozaveščanju o kibernetski varnosti«**. Dogodek je 27. novembra 2024 v Klubu Cankarjevega doma gostil 220 udeležencev iz celotne Evrope in postregel z vrhunskimi strokovnimi vsebinami s področja izobraževanja, komuniciranja in spreminjanja vedenjskih vzorcev uporabnikov.

Rdeča nit konference je bil človeški dejavnik kot najpogosteje izpostavljena šibka točka pri kibernetski varnosti. Predavanja so osvetlila, kako psihološki mehanizmi, kot so občutek zaupanja, strah ali pristranskost, vplivajo na uspešnost spletnih prevar. Strokovnjaki in raziskovalci s področja kibernetske varnosti so delili učinkovite pristope za krepitev varnostne kulture, od igrifikacije do jasne in osebno naslovljene komunikacije.

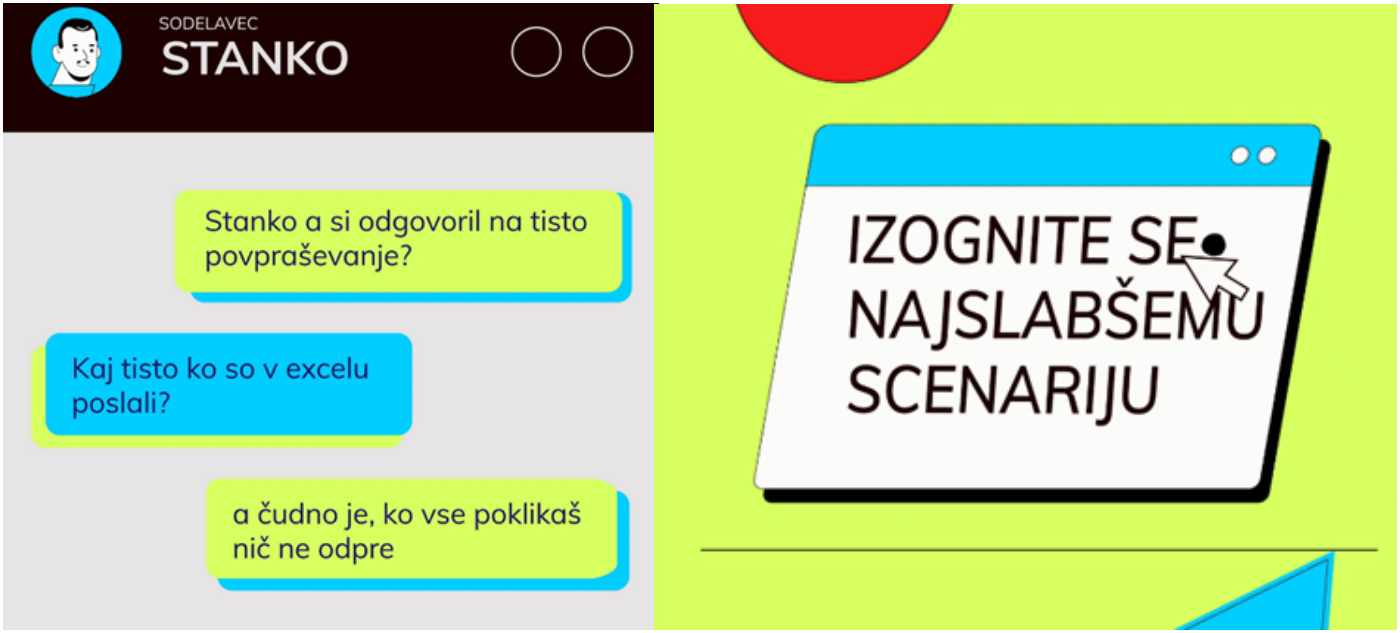
— Poudarek je bil na tem, kako pomembno je, da sporočila in varnostni napotki niso le strokovni, ampak tudi razumljivi in dostopni za različne ciljne skupine. Izpostavljena je bila tudi pomembna vloga vodstva, ki mora samo kazati visoke standarde varnostne kulture, da lahko to pričakuje od svojih zaposlenih.

Konferenca je odprla prostor za izmenjavo znanj med različnimi državami in sektorji ter potrdila, da so celostni pristopi k ozaveščanju, ki združujejo psihologijo, komunikacijo in tehnologijo, ključni za dolgoročno odpornost proti kibernetskim grožnjam.

PROMOCIJSKA KAMPANJA ZA SPLETNI TEČAJ VARNI V PISARNI

SI-CERT je leta 2021 zasnoval brezplačen spletni tečaj o osnovah informacijske varnosti za zaposlene Varni v pisarni. Spletni tečaj obravnava najpogostejša spletna tveganja, s katerimi se srečujejo manjša podjetja – od spletnih prevar in okužb z zlonamerno kodo do zlorab oglaševalskih računov, izgube podatkov in vdorov v informacijski sistem. Namenjen je tako zaposlenim kot vodstvu, vsebine pa so prilagojene različnim delovnim nalogam in procesom v podjetju.
Med septembrom in decembrom 2024 je bila načrtovana in izvedena promocijska kampanja za povečanje števila prijav na spletni tečaj Varni v pisarni. Zastavljeno merilo uspešnosti kampanje je bilo število novo registriranih uporabnikov spletnega tečaja, cilj pa bil dosežen še pred iztekom oglasne kampanje.

V promocijski kampanji smo s prilagojenimi kreativnimi rešitvami prikazovali realne situacije dopisovanja med zaposlenimi, ki so se soočili s kibernetskimi izzivi. Prav tako smo izpostavili negativne učinke kibernetskih napadov, ki lahko pomembno ogrozijo poslovanje podjetij.



Promocijska kampanja „Izognite se najslabšemu scenariju“

DECEMBRSKA KAMPANJA OSVETLILA POMEN MEDGENERACIJSKEGA SODELOVANJA

Decembra 2024 je bila v sklopu programa Varni na internetu predstavljena kampanja »Pomagajte svojim staršem«, namenjena uporabnikom, katerih starši ali drugi starejši svojci spadajo v starostno skupino nad 65 let.

— S sloganom »Pomagajte svojim staršem« smo nagovarjali k aktivni podpori starejših uporabnikov, ki so pogosto tarče spletnih prevar.

Uporabnike smo želeli spomniti, naj tako kot skrbijo za spletno varnost svojih otrok, pomislijo tudi na svoje starše, stare starše, tete in strice.

Kampanja je na družbenih omrežjih potekala decembra 2024 in je vključevala videe, ki prikazujejo povsem življenjske situacije – trenutke, ob katerih si lahko rečejo: »O, to se pa tudi meni dogaja!« Z znanima slovenskima igralcema smo pripravili video vsebine, ki prikazujejo vsakdanje situacije, ko starejši svojci potrebujejo pomoč pri zaščiti pred spletnimi prevarami, prepoznavanju lažnih sporočil ali zgolj nasvet glede varne hrambe gesel.

Ključne nasvete za zaščito pred spletnimi prevarami smo zbrali **v zgibanki 8 zlatih pravil spletne varnosti. Uporabniki so jo v sklopu kampanje lahko brezplačno naročili po pošti** in podarili svojim staršem, da so jo shranili na vidno mesto, na primer na hladilnik, kjer bo vedno pri roki. Na podlagi naročil smo poslali več kot 300 fizičnih izvodov. Zgibanka je na voljo tudi v digitalni obliki za prenos in tiskanje.

Zgibanka 8 zlatih pravil spletne varnosti

Poleg zgibanke z osnovnimi nasveti smo v letu 2024 razdelili tudi več kot 7000 priročnikov ABC varnosti, ki je v prvi vrsti namenjen starejšim uporabnikom spleta, v pomoč pa je tudi izvajalcem računalniških usposabljanj.

DOMAČE IN MEDNARODNO SODELOVANJE

Vpetost v mednarodno okolje in desetletja povezovanj s kolegi iz tujine so pogosto ključni za hitro ukrepanje, izmenjavo informacij in posledično zamejitev incidenta. SI-CERT je akreditiran skozi program Trusted Introducer (TI), ki od leta 2000 povezuje odzivne centre po vsem svetu. Trusted Introducer je koordinacijsko središče za izmenjavo informacij in dobrih praks ter upravlja seznam akreditiranih odzivnih centrov za obravnavo incidentov s področja kibernetske varnosti.

Skladno z Direktivo NIS2 je SI-CERT član mreže CSIRT; gre za povezavo, v kateri sodelujejo skupine CSIRT iz držav članic EU in CERT-EU. Je tudi član svetovnega združenja odzivnih in varnostnih centrov FIRST (Forum of Incident Response and Security Teams), član skupine nacionalnih odzivnih centrov pri CERT/CC in član delovne skupine evropskih odzivnih centrov TF-CSIRT.

SI-CERT je tudi sodelujoči partner v neprofitni mednarodni organizaciji Global Cyber Alliance, ki si prizadeva za krepitev kibernetske varnosti po vsem svetu. Ponosni smo, da lahko prispevamo k temu pomembnemu globalnemu prizadevanju. Global Cyber Alliance zasleduje tri glavne cilje: grajenje skupnosti, izmenjavo in dostopnost informacij in orodij ter merljivo zmanjšanje kibernetskih tveganj. Pri tem sodeluje s širokim naborom deležnikov, ki vključujejo vlade, podjetja, tehnološke ponudnike, akademske institucije, nevladne organizacije in posameznike. Skupnost, ki jo gradi organizacija, prinaša številne koristi. Poleg dostopa do orodij, praks in strokovnega znanja za izboljšanje kibernetske varnosti partnerji pridobijo tudi dostop do globalne mreže za sodelovanje in izmenjavo informacij. Sodelovanje v GCA partnerjem omogoča, da aktivno prispevajo k oblikovanju kibernetske politike in strategij ter se učinkovito odzovejo na nove kibernetske grožnje.

Uspešno zaključeni evropski projekti v letu 2024

V 2024 se je uspešno zaključil evropski projekt **»CyberSEAS: Kibernetska zaščita energetskih podatkovnih storitev (2021–2024)«,** financiran iz programa Obzorje 2020. Projekt je skupaj implementiralo 26 partnerjev iz zasebnega, javnega in energetskega sektorja iz osmih evropskih držav. Projekt CyberSEAS je naslavljal izzive kibernetske varnosti v evropskih energetskih sistemih ter bil osredotočen na izboljšanje splošne odpornosti energetskih dobavnih verig.

SI-CERT je v projektu sodeloval pri razvoju in izboljšanju procesov prijave in zaznave potencialnih incidentov ter pri iskanju rešitve za optimizacijo izmenjave občutljivih podatkov in informacij med prijavitelji in SI-CERT-om. V pilotnem delu projekta je SI-CERT sodeloval s platformo MISP in z izmenjavo podatkov o kibernetskih grožnjah ter s tem prispeval k širši uporabnosti končnih rešitev. V skladu s tem so bili scenariji pilotnih testiranj in programskih rešitev usklajeni in združljivi s platformo MISP, ki je široko razširjena v CSIRT-u in kibernetski varnostni skupnosti.

Rezultat projekta CyberSEAS je odprt in razširljiv ekosistem 30 prilagodljivih varnostnih rešitev, ki zagotavljajo učinkovito podporo za ključne dejavnosti, zlasti oceno tveganja, interakcijo s končnimi napravami, varen razvoj in uvajanje, varnostni nadzor v realnem času, izboljšanje veščin in ozaveščenost, certificiranje, upravljanje in sodelovanje.

Projekt je prejel sredstva iz programa Evropske unije za raziskave in inovacije Obzorje 2020 v okviru sporazuma o nepovratnih sredstvih št. 101020560.

Uspešne prijave prinašajo nove projekte

V letu 2024 sta bili uspešni dve prijavi projektov v okviru Programa za digitalno Evropo (DEP), in sicer na področju ukrepov uvajanja na področju kibernetske varnosti DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH. Oba projekta sta načrtovana v trajanju 36 mesecev in sta se začela izvajati v začetku leta 2025.

Prva prijava z naslovom **»ALiEnS-SOC, Umetna inteligenca za varnostno-operativni center slovenskega energetskega sektorja«** je nastala pod koordinacijo ELES d. o. o. in v konzorcij združuje 13 partnerjev. Poleg ELES-a so tu še podjetja za oskrbo z električno energijo iz Celja, Ljubljane, Maribora, Gorenjske in Primorske ter Telekom Slovenije d. d in INFORMATIKA d. d., SMARTIS d. o. o., TIKO PRO d. o. o., Urad Vlade Republike Slovenije za informacijsko varnost, ARNES SI-CERT in podjetje KONČAR -Digital d. o. o. iz sosednje Hrvaške.

Projekt ALiEnS-SOC si bo prizadeval vzpostaviti robusten kibernetsko-varnostni okvir, ki vključuje sistem na osnovi umetne inteligence s polnim potencialom za repliciranje, pilotno preizkušen in potrjen v Nacionalnem varnostno-operativnem centru za elektroenergetiko (SOC). Njegova vrednost bo v izboljšanem zaznavanju, prestrezanju in odzivanju na varnostne incidente in ranljivosti, zmanjšanju tveganj ter povečanju hitrosti odzivanja in operacij. Prinaša pa tudi učinkovitejšo komunikacijo in izmenjavo izkušenj in informacij med deležniki za krepitev kibernetske varnosti SOC-ov na nacionalni ravni in ravni EU. Projekt vključuje napredne pristope umetne inteligence in kibernetskega obveščanja (CTI). Prilagojen je posebnim zahtevam okolij informacijske in operativne tehnologije. Ta integracija zagotavlja celovito zaznavanje groženj, odzivanje na incidente in preprečevanje goljufij ter znatno izboljšuje sposobnost predvidevanja, zaznavanja in nevtralizacije kibernetskih groženj, s čimer ščiti nemoteno delovanje in kibernetsko odpornost kritične infrastrukture.

V okviru projekta ALiEnS-SOC je za SI-CERT za obdobje treh let predvidenih 147.125,00 € (tj. 50 % sofinanciranje od EU, 50 % lastno udeležbo pa zagotavlja URSIV).

Projekt, financiran v okviru pogodbe o dodelitvi sredstev št. 101190349, podpira Evropski strokovni center za kibernetsko varnost.

Druga uspešna prijava nosi naslov **»INTERCEPT – Platforma za deljenje informacij o kibernetskih grožnjah in incidentih«**. Nastala je pod koordinacijo T-2, d. o. o. in v konzorcij združuje Pošta Slovenije d. o. o., TIKO PRO d. o. o., ARNES SI-CERT in hrvaški KONČAR - Digital d. o. o.

Splošni cilj projekta INTERCEPT je izboljšanje SOC-ov iz Slovenije in Hrvaške z razvojem potrebne tehnologije in vzpostavitvijo čezmejnega sodelovanja na področju kibernetske varnosti v obliki skupne platforme za lažje soočanje s kibernetskimi grožnjami. V okviru projekta bo vsak partner integriral platformo MISP v svoje notranje procese, kar bo spodbudilo delitev oz. izmenjavo znanja in čezmejno sodelovanje. S konsolidacijo virov in strokovnega znanja si projekt INTERCEPT prizadeva opolnomočiti SOC partnerje konzorcija za učinkovitejše reševanje kibernetskih izzivov in proaktivno obvladovanje novih groženj. Platforma TSP, ki bo tako nastala, bo omogočala izmenjavo obogatenih podatkov med partnerji in s tem izboljšala skupne kibernetske varnostne ukrepe. V okviru projekta ALiEnS-SOC je za SI-CERT za obdobje treh let predvidenih 82.390,00 € (tj. 50 % sofinanciranje od EU).

Co-funded by the European Union

Projekt, financiran v okviru pogodbe o dodelitvi sredstev št. 101190460, podpira Evropski strokovni center za kibernetsko varnost

IZMENJAVA INOFRMACIJ O KIBERNETSKIH GROŽNJAH

Naraščajoča potreba po izmenjavi informacij za zaščito sistemov je prisotna tako v mednarodni kot slovenski kibernetski skupnosti. Hiter prenos informacij o kibernetskih grožnjah, njihova samodejna obdelava in učinkovitejša zaščita omrežij so danes predpogoji za zagotavljanje kibernetske varnosti. Veliko varnostnih strokovnjakov išče rešitve za pridobivanje informacij prek javnih in plačljivih virov, ki oskrbujejo ključne sisteme v omrežju z informacijami o najnovejših tveganjih v kibernetskem prostoru. Kot vedno pa obstajajo alternativne možnosti; ena od njih je razvita v okviru več kot desetletja starega projekta Malware Information Sharing Platform (v nadaljevanju MISP).

Uporaba platforme MISP v Sloveniji

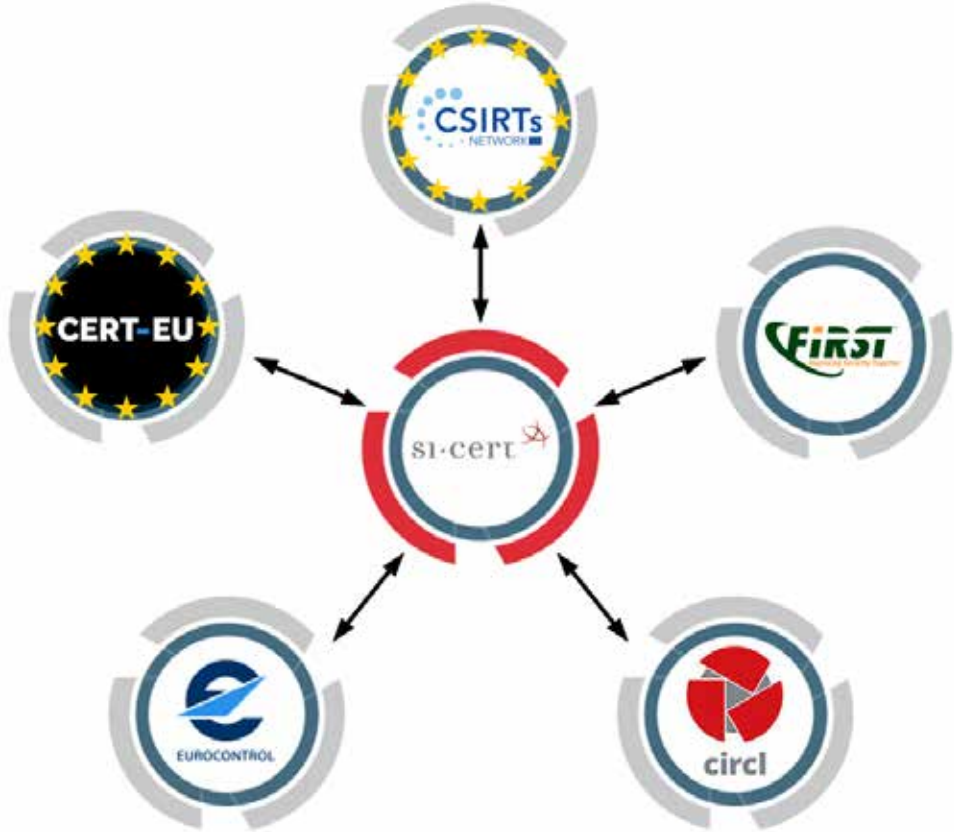
Stičišče MISP v Sloveniji upravlja SI-CERT, kjer širimo zavedanje o pomembnosti izmenjave informacij med lokalnimi deležniki ravno prek platforme MISP. Zgodba uporabe platforme MISP je na SI-CERT-u stara skoraj deset let; posledično je v tujini izmenjava kibernetskih groženj prek platforme že dodobra razširjena in velja za nujnost v okoljih, kjer se ukvarjajo s preučevanjem ali omejevanjem kibernetskih groženj. Informacije o kibernetskih grožnjah, izmenjane s tujimi deležniki, so pripomogle k obogatitvi marsikatere preiskave, ki jo je vodil SI-CERT, ter so prinesle ključne informacije za ugotavljanje vzrokov in boljšo zaščito pred kibernetskimi grožnjami.

Uporabnost platforme temelji ravno na široki skupnosti uporabnikov, ki redno nesebično delijo podatke o odkritih grožnjah v svojih omrežjih. Sodelujejo z zavedanjem, da je le na tak način mogoče ustvariti širšo zgodbo iz ugotovljenih analiz incidentov in dogodkov, saj je tudi v tem primeru zgolj vzpostavitev skupne obrambe najboljša rešitev za zaščito pred kibernetskimi napadi. SI-CERT spodbuja uporabo podatkov, ki so deljeni na platformi, kot tudi dodajanje informacij, zaznanih v omrežjih povezanih organizacij. Takšno solidarno delovanje bo prineslo lažje razumevanje o razširjenosti kibernetskih groženj in dodatno obogatilo vedenje o grožnjah samih.

Izmenjava podatkov z mednarodnimi partnerji

Izmenjava podatkov z mednarodnimi partnerji poteka prek povezav MISP-a, ki obsegajo bogat nabor virov informacij. Med njimi sta sodelovalno okolje za izmenjavo groženj v okviru **mreže evropskih odzivnih centrov ENISA CSIRTs Network ter evropska kontrola zračnega prometa EATM-CERT**, če izpostavimo le nekaj priznanih partnerjev.

Tu so še neposredne izmenjave s priznanimi deležniki, med drugim **CIRCL in CERT-EU. Na mednarodni ravni poteka izmenjava prek svetovnega združenja odzivnih skupin FIRST.** Vsi ti viri informacij o kibernetskih grožnjah SI-CERT-u zagotavljajo širšo sliko o svetovnih kibernetskih grožnjah.



Izmenjava podatkov z mednarodnimi partnerji prek povezav MISP-a, ki obsegajo bogat nabor virov informacij.

Prednosti vključitve na platformo MISP

V slovenskem prostoru že poteka izmenjava informacij s posameznimi deležniki prek platforme MISP. Ti z vključitvijo pridobijo dragocene podatke, ki jim, v povezavi s sistemom za pregled in zbiranje varnostnih informacij SIEM, omogočajo boljšo varnost nadzorovanih omrežij. **Prednost tovrstne povezave je tudi hipna pridobitev podatkov o grožnjah, v primerih groženj, vnesenih s strani SI-CERT-a, celo hitreje kot prek drugih, morda plačljivih seznamov**, saj pri predaji informacij ni vpletenih posrednikov in nepotrebnega preverjanja. Atributi, deljeni prek platforme MISP, namreč lahko vsebujejo oznako, ki opredeljuje indikatorje okužbe oz. t. i. IoC podatke kot primerne za omrežno pregledovanje in blokiranje. Tako lahko v primeru zaznanih korelacij s podatki, pridobljenimi s pomočjo MISP-a, ugotovijo sum na morebitne varnostne grožnje znotraj omrežja ali okužene delovne postaje. Če organizacija sama s preučitvijo varnostnega incidenta pridobi t. i. IoC podatke, jih lahko vnese v MISP in jih tako deli z skupnostjo.

S platformo MISP SI-CERT aktivno postavlja nove mejnike na področju varnosti v slovenskih omrežjih ter podaja informacije, ki lahko z ustrezno implementacijo pomagajo vsem državljanom.

DELJENJE ZNANJA S ŠIRŠO SKUPNOSTJO

Zaposleni na SI-CERT-u vsako leto izvedemo številna predavanja ter strokovno znanje in izkušnje delimo na okroglih mizah in delavnicah. **V letu 2024 smo sodelovali na 60 tovrstnih dogodkih, ki so bili namenjeni različnim javnostim.** Osredotočamo se na teme, ki so nam blizu: odzivanje na kibernetske incidente in njihovo preiskovanje, obravnava ranljivosti, deljenje informacij o kibernetskih grožnjah, izobraževanje zaposlenih in ozaveščanje javnosti. Z objavo varnostnih opozoril, novic in poglobljenih tehničnih zapisov na spletnem mestu www.cert.si redno seznanjamo strokovno javnost z opaženimi trendi na področju kibernetske varnosti in s tem povezanimi grožnjami. Urejamo dva novičnika, *SI-CERT Odziv* za strokovno javnost in *Varne novice*, ki je namenjen širši javnosti z namenom seznanjanja z novimi spletnimi goljufijami, usmerjenimi na posameznike in mala podjetja. Vsebine objavljamo tudi na družbenih omrežjih. Naša dolgoletna vpetost in vloga v mednarodni skupnosti CSIRT pa nam omogoča tudi deljenje izkušenj sodelovanja skupin CSIRT v EU in v neposredni regiji.

Podpora skupinam CSIRT Zahodnega Balkana

SI-CERT od leta 2011 dalje aktivno pomaga pri vzpostavljanju in mentoriranju skupin CSIRT v regiji Zahodnega Balkana. Ta je dolga leta na zemljevidu Evrope predstavljal sivo liso z vidika odzivanja na incidente. Sodelovanje skupin CSIRT je ob obravnavi incidenta nujno, pri tem pa seveda potrebujemo sogovornika na drugi strani. Slika je danes veliko boljša – kljub težavam, ki so specifične za omenjeno regijo, imamo zemljevid dopolnjen z nacionalnimi in vladnimi odzivnimi skupinami CSIRT tako rekoč v celotni regiji. V letu 2024 smo se posvečali bolj usmerjenim strokovnim temam in praktičnim primerom obravnave incidentov, kot svetovalci pa člani SI-CERT-a sodelujemo tudi v programu *EU Cyber Balkans.*

Dvodnevna delavnica o učinkovitem komuniciranju

Poleg izjemne tehnične podkovanosti je sposobnost jasnega, učinkovitega in strateškega komuniciranja še ena od zahtev za uspešno delovanje odzivnih centrov. Strokovna sodelavka SI-CERT-a je zato za predstavnike različnih ministrstev in institucij iz Albanije, Bosne in Hercegovine, Kosova, Črne gore, Severne Makedonije in Srbije izvedla intenzivno, dvodnevno delavnico z naslovom *Razvoj učinkovite strategije komuniciranja in odnosov z mediji za ekipe za odzivanje na kibernetske incidente.* Delavnica je potekala 28. in 29. novembra 2024 v City Hotelu v Ljubljani, v okviru projekta EU *Cyber Balkans* za krepitev kibernetske varnosti v državah Zahodnega Balkana.

Cilj delavnice je bil udeležencem, odgovornim za komuniciranje v svojih institucijah, predstaviti ključne elemente učinkovite komunikacijske strategije in odnosov z mediji. Poseben poudarek je bil na pomenu strukturiranega načrta odnosov z mediji kot pomembnega kazalca zmogljivosti in zrelosti odzivne skupine, ozaveščanju uporabnikov o kibernetski varnosti ter o osnovah kriznega komuniciranja. Program je vključeval teoretične predstavitve in praktične naloge, kot so priprava komunikacijskih vsebin, oblikovanje kampanj ozaveščanja ter priprava izjav za javnost ob kibernetskem incidentu.

Naslov publikacije: Poročilo o kibernetski varnosti za leto 2024
Avtor publikacije: Nacionalni odzivni center za kibernetsko varnost SI-CERT
Leto izida: 2025
Naklada: 540 izvodov
Založnik: Akademska in raziskovalna mreža Slovenije
Oblikovanje in prelom: MONU – design biro
Vsa letna poročila o kibernetski varnosti v Sloveniji, ki jih izdajamo pri centru SI-CERT, so dostopna na naslovu www.cert.si/letna_porocila/.

si·cert

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

cert@cert.si

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

www.cert.si

@SI-CERT, Slovenian National Computer Emergency Response Team
sicert
@sicert