



Poročilo o kibernetški varnosti za leto 2025

Nacionalni odzivni center
za kibernetško 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

 @sicert

Ozaveščanje javnosti na področju informacijske varnosti

www.varninainternetu.si

 varninainternetu

 @varninanetu

 varninainternetu

SI-CERT je financiran s sredstvi
Urada Vlade Republike Slovenije za informacijsko varnost.



Kazalo

KLJUČI KRALJESTVA	4
KLJUČNE ŠTEVILKE V LETU 2025	6
LETO 2025 NA DLANI	8
PREDSTAVITEV ODZIVNEGA CENTRA SI-CERT	10
Kdaj prijaviti incident?	13
DOMAČE IN MEDNARODNO SODELOVANJE	14
Si-cert in evropski projekti v letu 2025	16
Uporabnost seznamov SI CERT za zaščito sistemov in vpogled v njihovo rabo	19
VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALCI	24
Vrste incidentov	26
Incidenti skozi leta	27
Odzivni čas SI-CERT	28
IZPOSTAVLJENE TEME V LETU 2025	34
30 let pomoči, zaupanja in grajenja kibernetske skupnosti	35
NACIONALNI PROGRAM OZAVEŠČANJA O KIBERNETSKI VARNOSTI	38

Uvodnik

KLJUČI KRALJESTVA

Že vrsto let v svojih poročilih navajamo strmo rast števila objavljenih ranljivosti. Velja pa omeniti tudi trend, ki vzbuja skrb vsaj zadnjih pet let: kritične ranljivosti naprav, ki so dejansko prva obrambna linija naših notranjih omrežij. V skupnosti CSIRT lahko spremljamo že kar sarkastične pripombe podjetij v smislu: »Hej, petek je, kje je nov O-day za ...« Imena ne bom navedel, seveda.

Kako je mogoče, da podjetja, ki jim tako rekoč predamo ključne svojega kraljestva, bolje ne poskrbijo za izpolnitev svojih obljub iz oglasov? Težko vprašanje, a k temu verjetno prispeva konkurenčni boj in posledično nižanje stroškov, ki se prelije v manj kakovosten razvoj in skrajševanje faz načrtovanja in varnostnega preverjanja. Zaradi istega razloga velika podjetja kupujejo manjše ponudnike varnostnih storitev in tako pridobijo njihovo celotno programsko kodo, zmanjka pa časa za njen temeljiti pregled (pogosto pa je to še tečno opravilo). Zna biti, da je težava tudi odsotnost odgovornosti proizvajalcev za težave, ki jih morate potem čez noč, ko udari nov O-day, reševati skupaj z nami.

Boste rekli, da je vse to posledica generativne umetne inteligence, pri kateri spremljamo uspeh specializiranih modelov, ki ranljivosti odkrivajo kot po tekočem traku? Da in ne. Zgodba sega namreč že v čas pred tem. Takrat smo sumili, da veliki organizirani kriminal in državno podprti akterji veliko investirajo ravno v iskanje ranljivosti omenjenih produktov, da bi si pridobili dostop do dragocenih ciljev. Za nekatere ranljivosti smo tudi upravičeno začudeni, da se vedno znova pojavijo v teh specializiranih produktih (recimo path traversal). Je pa res, da nova UI-orodja pomenijo bistven preskok, tudi če skušamo odgrniti vse plasti marketinga, ki spremljajo vodilne produkte LLM. Trend spremljamo v skupnosti in za zdaj še iščemo odgovore nanj.

Drvimorej v brezno, kjer upanje izgine? Ne, le pomembnejše postaja tisto, kar vemo že sicer. Preverimo, kakšna bo škoda ob neupravičenem dostopu. Do kam lahko vdiralci pridejo, kje pa jim postavimo nove prepreke? Kako hitro se bomo lahko odzvali in spet zagnali poslovanje? EU želi z novimi akti in direktivami prispevati k strožjim pogojem za proizvajalce, vendar vemo, da se zakonodaja zaradi svoje narave vpeljuje sorazmerno počasi, ukrepati je pa treba hitro. Bo vodstvo podjetja pripravljeno v krizi hitro zamenjati ključne zaščitne komponente omrežja?

Da pa ne bom omenjal zgolj velikih proizvajalcev varnostnih rešitev: ste ključne kraljestva z dostopom VPN razdelili tudi svojim pogodbenim izvajalcem? Ali še imate evidenco o tem, kdo vse jih ima, in ali ste predhodno razmislili, do česa vse lahko z vašim dovoljenjem dostopajo? To je namreč postal glavni vstopni vektor za izsiljevalske napade s krajo podatkov in za onemogočanje vaših sistemov.



Gorazd Božič
Vodja SI-CERT



KLJUČNE ŠTEVILKE V LETU 2025

6196
incidentov

778
od tega
zahtevnejših

35% porast incidentov

&

44% porast prejetih prijav

1995

1100

zlonamernih domen na
zadržalnem seznamu

159
novinarskih vprašanj

5337
novih tečajnikov na portalu
Varni v pisarni

5000+
naročnikov novice
SI-CERT Odziv

6
izvedenih
spletnih seminarjev

JAN

Obveščali smo o množičnem ustvarjanju uporabniških računov na platformi Telegram s slovenskimi telefonskimi številkami, pri čemer računov niso ustvarili uporabniki teh števil. Istočasno je prihajalo tudi do prevzemov obstoječih Telegramovih računov. Točnega načina teh zlorab nismo ugotovili, najverjetneje pa so napadalci pridobili dostop do enega od ponudnikov, ki jih je Telegram uporabljal za pošiljanje potrditvenih kod preko SMS.

MAR

Mesec, v katerem smo prejeli največ prijav, in sicer 1463 oz. v povprečju 47 vsak dan. Dnevno povprečje števila prejetih prijav za celotno leto 2025 znaša 37,8.

FEB

Obveščali smo o pojavu zanimivih omrežnih napadov, katerih cilj je bila okužba računalnika. Napadalci so na spletna mesta nameščali zlonamerno kodo, ki je obiskovalcem spletnega mesta prikazovala t. i. CAPTCHA poziv, ki ga je bilo treba rešiti s pritiskom določene kombinacije tipk na tipkovnici. Kombinacija pritiskov na te tipke je na sistem namestila zlonamerno kodo, največkrat iz družine kradljivcev podatkov Lumma.

JUL

Microsoft je izdal varnostno obvestilo o kritični ranljivosti Microsoft SharePoint z oznako CVE-2025-53770. Mnogi varnostni strokovnjaki so jo opredelili kot ranljivost leta 2025 z najresnejšimi posledicami, saj je omogočala izvajanje poljubne kode brez avtentikacije. Množica aktivnih strežnikov po vsem svetu je omogočala masovno izrabo, vpetost ranljivih strežnikov v omrežno infrastrukturo organizacij pa hitro zlorabo celotne domene.

AVG

Cisco je izdal posodobljeno varnostno obvestilo o izkoriščanju sedem let stare ranljivosti Cisco Smart Install CVE-2018-0171 s strani državno podprtih akterjev. Čeprav je šlo za ranljivost iz leta 2018, je avgusta 2025 postalo jasno, da je še vedno množično prisotna v realnih omrežjih, predvsem na starejših neposodobljenih stikalih Cisco. Aktivne zlorabe teh naprav smo zaznavali tudi v Sloveniji.

SEP

Zakon o informacijski varnosti je SI-CERT določil za koordinatorskega v postopku usklajenega razkrivanja ranljivosti v Republiki Sloveniji. Koordinator deluje kot zaupanja vreden posrednik med najditeljem ranljivosti ter proizvajalcem oz. ponudnikom storitev. Septembra 2025 smo na SI-CERT prejeli prvo prijavo ranljivosti v tej vlogi.

LETO 2025 NA DLANI

APR

Pričeli smo s serijo spletnih seminarjev, na katerih pokrivamo različne teme. V letu 2025 smo izvedli šest seminarjev, prvega aprila 2025 z naslovom »Kibernetska varnost za spletne trgovce«.

MAY

V Ljubljani je potekal posvet o izobraževanju zaposlenih o kibernetski varnosti, ki ga je organiziral SI-CERT. Dogodek je pod naslovom »Novi pristopi za nove grožnje« združil strokovnjake s področja kibernetske varnosti, kadrovskih služb ter izobraževanja. Šlo je za prvi tovrstni strokovni dogodek v Sloveniji.

OKT

SI-CERT obeleži 30 let delovanja – tri desetletja odzivanja na kibernetske incidente, pomoči in grajenja kibernetske skupnosti. Jubilejni dogodek smo obeležili z odprtjem razstave »Hakerji – kibernetska (ne)varnost« v Računalniškem muzeju. Mesec prej smo na konferenci INFOSEK prejeli tudi nagrado za življenjsko delo na področju informacijske varnosti.

DEC

Tik pred prazniki smo obravnavali izredno obsežen phishing napad pod krinko nedostavljene pošiljke v obliki lažnih sporočil iMessage. V napadu je bilo uporabljenih več kot 70 različnih, na novo registriranih domen. Napadalci so izkoriščali čas, ko je zelo veliko ljudi pričakovalo dostavo pošiljke, zato je bil napad precej uspešen. Na SI-CERT se je obrnilo večje število oškodovanih uporabnikov.

JAN

Državni zbor Republike Slovenije je sprejel nov Zakon o informacijski varnosti (ZInfV-1), ki v slovenski pravni red prenaša evropsko direktivo NIS2. Med ključne novosti zakona spadajo bistveno povečanje števila zavezancev, obvezno upravljanje kibernetskih tveganj, strožji režim prijave incidentov ter okrepljena vloga skupin CSIRT in Urada Vlade RS za informacijsko varnost (URSIV).

NOV

Obveščali smo o pojavu naprednih phishing napadov na spletne banke podjetij z elementom telefonskega klica. Začetnemu phishing sporočilu je sledil ponarejen klic iz banke, pri katerem so napadalci žrtve prepričali, da jim bodo pomagali pri posodobitvi programske opreme za spletno bančništvo. Po pridobitvi dostopa do računalnika in po prijavi žrtve v spletno banko so denarna sredstva lahko prenakazali na tuje račune.



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 Javnega zavoda Arnes. Njegove primarne naloge so 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.

Novi Zakon o informacijski varnosti (ZInfV-1), sprejet maja 2025, v slovenski pravni red prenaša evropsko direktivo (EU) 2022/2555 (NIS 2) in določa pravila za izboljšanje varnosti omrežij ter informacijskih sistemov. Skladno z 59. členom ZInfV-1 je **SI-CERT pristojen za obravnavo incidentov**, ki jih prijavijo zavezanci iz prvega odstavka 6. člena ZInfV-1, razen subjektov javne uprave na državni in lokalni ravni ter ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave. **Kot ključne naloge na SI-CERT izpostavljamo sprejem prijav incidentov, ki jih prijavijo zavezanci, in nudenje 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 kibernetских incidentov nacionalni skupini CSIRT, so tri skupine subjektov:

1. Zavezanci iz prvega odstavka 6. člena ZInfV-1, razen subjektov javne uprave na državni in lokalni ravni ter ponudnikov storitev zaupanja, ki jih izvajajo subjekti državne uprave, morajo na SI-CERT priglasiti **vse incidente, ki imajo pomemben vpliv na zagotavljanje njihovih storitev**. Incident se šteje za pomembnega, če je zavezancu povzročil ali bi mu lahko povzročil resne operativne motnje pri opravljanju storitev ali finančne izgube, ali pa je vplival ali bi lahko vplival na druge fizične ali pravne osebe s povzročitvijo precejšnje premoženjske ali nepremoženjske škode.

2. Zavezanci po Zakonu o varstvu osebnih podatkov (ZVOP-2): Zakon o varstvu osebnih podatkov prenaša evropsko Splošno uredbo o varstvu podatkov (GDPR) 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 ukrepih za obvladovanje tveganj **in priglasitev incidentov iz zakona, ki ureja informacijsko varnost, ki se nanašajo na bistvene subjekte**, če upravljavec glede teh obdelav ni dolžan izvajati ukrepov po zakonu, ki ureja informacijsko varnost.

3. V skladu z Uredbo o izvajanju uredbe (EU) o digitalni operativni odpornosti za finančni sektor morajo finančni subjekti o večjih incidentih, povezanih z IKT, poročati pristojnim organom in skupinam za odzivanje na incidente s področja računalniške varnosti (CSIRT). Prijava pristojnemu nadzornemu organu hkrati pomeni tudi prijavo na pristojno skupino CSIRT, zato posebno obveščanje SI-CERT ni potrebno.

Zavezanci lahko skladno s prvim odstavkom 35. člena ZInfV-1 na SI-CERT prijavijo tudi incident, ki ne spada v kategorijo pomembnih incidentov. Taka prijava se obravnava kot **prostovoljna priglasitev**.

Prav tako lahko tudi vsi preostali poslovni subjekti, javne ustanove in fizične osebe podajo prostovoljno prijavo incidenta na SI-CERT. Namen prijave je strokovna pomoč pri identifikaciji težave, pomoč pri njeni odpravi, zamejitvi in odpravi posledic.

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 kibernetских incidentov se lahko obrnejo subjekti, ki jim to predpisuje zakon, prav tako tudi druge pravne in fizične osebe.

KDAJ PRIJAVITI INCIDENT?

Primer incidenta

Okužba računalnika
(izsiljevalski virusi, bančni trojanski konji, ciljani napadi, agenti za pošiljanje neželene elektronske pošte)

Opažen vdor v strežnik
(razobličenje, zloraba podatkovnih zbirk, namestitvev prikritih orodij storilca)

Phishing elektronska sporočila
(potvorjena elektronska sporočila, ki vas napeljujejo, da geslo vpišete na lažni spletni strani)

Napad onemogočanja
(poplava s prometom, napad na storitev ali spletno aplikacijo z namenom njenega onemogočanja)

Ranljive ali izpostavljene storitve
(vmesniki za upravljanje spletnih storitev, upravljanje naprav ali industrijskih procesov, spletnih kamer ipd., ranljiva omrežna infrastruktura, ki omogoča napade onemogočanja)

Izguba gesel ali kraja omrežne identitete
(zloraba prek phishing napada ali okužbe računalnika)

Pričakovane dejavnosti centra SI-CERT

Pomoč pri odstranjevanju okužbe in njenih posledic, analiza vzorca in korelacija z do zdaj znanimi grožnjami. Svetovanje o ukrepih za sanacijo stanja.

Iskanje izrabljene varnostne luknje ali ranljivosti, pomoč pri opredeljevanju posledic in vira vdora, analiza sledi na zlorabljenih sistemih, nasveti za odstranjevanje škode in zaščito.

Odstranjevanje in označevanje lažnih spletnih mest. Prepoznavanje širših in ciljanih napadov, obveščanje medijev in javnosti, sodelovanje z bančnim sektorjem in ponudniki storitev.

Ocena o uporabljenih sredstvih za napad, opredelitev mogočih zaščitnih ukrepov, poskus onemogočanja botneta ter obveščanje ponudnikov o zlorabljeni infrastrukturi in njeni zaščiti.

Obveščanje skrbnikov, svetovanje pri nastavitvah in omejevanju dostopa, preiskovanje zlorabe storitve.

Svetovanje pri ponovnem prevzemu računov, dodatnih zaščitnih ukrepov in mogoči identifikaciji storilca.



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 s programom 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 kibernetске 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 kibernetске varnosti po vsem svetu. Global Cyber Alliance sledi trem glavnim ciljem: grajenje skupnosti, izmenjava in dostopnost informacij in orodij ter merljivo zmanjšanje kibernetских tveganj. Pri tem sodeluje s širokim spektrom 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 kibernetске varnosti partnerji pridobijo tudi dostop do globalne mreže sodelovanja in izmenjave informacij. Sodelovanje v GCA partnerjem omogoča, da aktivno prispevajo k oblikovanju kibernetске politike in strategij ter se učinkovito odzovejo na nove kibernetске grožnje.



SI-CERT IN EVROPSKI PROJEKTI V LETU 2025

V vlogi nacionalne skupine CSIRT se SI-CERT vključuje tudi v projektne konzorcije, ki si prizadevajo za razvoj novih tehnologij, digitalizacijo, kibernetsko varnost v državah članicah EU in podpirajo področno sodelovanje na nacionalni in mednarodni ravni. Tako so bila v preteklih letih pridobljena sredstva, ki so SI-CERT omogočila izboljšati tehnično opremljenost ter s tem tudi zahtevano skladnost z nacionalnimi in evropskimi standardi in zakonodajo. Poleg proračunskih sredstev, ki jih za delovanje SI-CERT zagotavlja URSIV, so pridobljena evropska sredstva dodatna sredstva za tehnični razvoj, mednarodno sodelovanje in mreženje ter strokovno promocijo SI-CERT.

Dodatna sredstva, možnost sodelovanja pri tehničnem razvoju ter mreženje in mednarodno povezovanje so botrovali odločitvi o sodelovanju v dveh pretežno slovenskih konzorcijih, ki sta nato v letu 2024 uspešno kandidirala na razpisu iz Programa za digitalno Evropo (DEP).

SI-CERT tako od začetka leta 2025 sodeluje v dveh projektih DEP, ki sta bila odobrena v okviru razpisa DIGITAL-ECCC-2024-DEPLOY-CYBER-06-ENABLINGTECH, ki neposredno naslavlja razvoj in uporabo naprednih sistemov ter orodij za kibernetsko varnost, ki temeljijo na umetni inteligenci in drugih ključnih tehnologijah. Osrednji poudarek razpisa je krepitev zmogljivosti tako varnostno-operativnih centrov kot nacionalnih čezmejnih platform za učinkovitejše odkrivanje, analizo in preprečevanje kibernetskih groženj ter incidentov.

Program za digitalno Evropo (2021–2027) je ključni program financiranja EU za pospeševanje digitalne preobrazbe, ki podpira podjetja, javno upravo in državljane z naložbami v superračunalništvo, umetno inteligenco, kibernetsko varnost in digitalne spretnosti.



Projekt **ALiEnS-SOC** – »Umetna inteligenca za varnostno-operativni center slovenskega energetskega sektorja« izvaja konzorcij trinajst projektnih partnerjev v koordinaciji ELES d.o.o. V konzorcij so vključena podjetja za oskrbo z električno energijo iz Celja, Ljubljane, Maribora, Gorenjske in Primorske ter Telekom Slovenije d.d., 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, Digitalna d.o.o. iz Hrvaške.

Projekt ALiEnS-SOC si prizadeva vzpostaviti robusten kibernetsko-varnostni okvir, ki vključuje sistem na osnovi umetne inteligence s polnim potencialom za ponovno uporabo, pilotno preizkušen in potrjen v Nacionalnem varnostno-operativnem centru za elektroenergetiko. Njegova vrednost bo v izboljšanjem zaznavanju, prestrezanju in odzivanju na varnostne incidente in ranljivosti, v zmanjšanju tveganj ter povečanju hitrosti odzivanja in operacij, poleg učinkovitejše komunikacije, izmenjave izkušenj in informacij med deležniki. Namenjen je krepitvi kibernetske varnosti varnostno-operativnih centrov na nacionalni in ravni EU. Projekt, usmerjen v izboljšanje kibernetske varnosti nacionalnega varnostno-operativnega centra za elektroenergetski sektor, je strateško zasnovan za reševanje operativnih in tehničnih izzivov kibernetske varnosti.

V okviru projekta ALiEnS-SOC je ob 50-odstotnem evropskem sofinanciranju za SI-CERT v triletnem obdobju predvidenih 294.250 evrov (oz. 50 %, kar znaša največ 147.125 evrov).



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

PROJEKTI V TEKU



Projekt **INTERCEPT** – »Platforma za deljenje informacij o kibernetskih grožnjah in incidentih« izvaja koordinator projekta T-2, d.o.o. v sodelovanju s Pošto Slovenije d.o.o., TIKO PRO d.o.o., ARNES – SI-CERT in hrvaškim podjetjem KONČAR - Digitalna d.o.o.

Splošni cilj projekta INTERCEPT je izboljšanje delovanja dveh varnostno-operativnih centrov iz Slovenije in Hrvaške. V ta namen se v okviru projekta razvija potrebna tehnologija in utrjuje čezmejno sodelovanje na področju kibernetske varnosti, in sicer v obliki skupne platforme za izmenjavo groženj, ki bo v pomoč pri lažjem spopadanju s kibernetskimi grožnjami. V okviru tega projekta partnerji integrirajo platformo MISP v svoje notranje procese, kar bo spodbudilo in olajšalo izmenjavo podatkov, znanja in izboljšalo čezmejno sodelovanje. Projekt INTERCEPT bo tako prispeval k opolnomočenju konzorcijskih partnerjev in njihovih varnostno-operativnih centrov ter k učinkovitejšemu reševanju kibernetskih izzivov in bolj proaktivnemu obvladovanju novih groženj. Nastajajoča platforma INTERCEPT bo omogočala izmenjavo obogatitvenih podatkov med partnerji in s tem izboljšala skupne kibernetske varnostne ukrepe.

V okviru projekta INTERCEPT je ob 50-odstotnem evropskem sofinanciranju za SI-CERT v triletnem obdobju predvidenih 164.780 evrov (oz. 50 %, kar znaša največ 82.390 evrov).



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



Novi projekt VANTAGE – »Ocenjevanje ranljivosti in avtomatizirano testiranje za izboljšave na globalni ravni«



V letu 2025 je bil v okviru razpisa DIGITAL-ECCC-2024-DEPLOY-CYBER-07-KEYTECH iz programa DEP 2024 potrjen tudi projekt **VANTAGE – »Ocenjevanje ranljivosti in avtomatizirano testiranje za izboljšave na globalni ravni«**. Projekt bo zaživel na začetku leta 2026 ter pod grškim koordinatorjem Diadikasia Business Consulting SA združuje trinajst projektnih partnerjev s španskih, italijanskih in danskih univerz, javnih zavodov iz Slovenije in iz zasebnih neprofitnih organizacij ter profitnih organizacij in podjetij iz Italije, Belgije, Grčije, Estonije in Bolgarije. Iz Slovenije poleg SI-CERT sodeluje tudi Institut Jožef Stefan.

Projekt VANTAGE je namenjen izboljšanju odkrivanja ranljivosti in preiskovanja kibernetских incidentov v omrežjih, sistemih in aplikacijah. Projekt se osredotoča na kibernetске zmogljivosti naslednje generacije, podprte z umetno inteligenco, za varnostne operativne centre, skupine za odzivanje na incidente na področju računalniške varnosti (CSIRT), podjetja in relevantne institucionalne deležnike. V okviru projekta bo razvita integrirana platforma, ki bo združevala večagentno, večmodelno in multimodalno umetno inteligenco, avtomatizirano ocenjevanje ranljivosti in penetracijsko testiranje, preiskave incidentov, OSINT in forenzične podporne zmogljivosti, hkrati pa bo izvajala izpopolnjene kontrole in varovalke, usklajene z veljavno pravno, etično in varnostno zahtevo, vključno s Splošno uredbo o varstvu podatkov, Zakonom EU o umetni inteligenci, direktivo NIS2, Zakonom o kibernetски odpornosti in drugimi relevantnimi pravnimi okviri. Večagentna arhitektura umetne inteligence bo omogočila avtonomno koordinacijo, dinamično prilagajanje in poglobljeno analitično sklepanje ter s tem manj ročnih opravil, izboljšano hitrost in natančnost odzivov na kibernetске grožnje za sodobne sisteme SOC in CSIRT. Orodja za stalno spremljanje bodo omogočala sprotno spremljanje dogajanja, zaznavanje nepravilnosti ter samodejno obveščanje o morebitnih varnostnih incidentih.

V okviru projekta VANTAGE je ob 50-odstotnem evropskem sofinanciranju za SI-CERT v triletnem obdobju predvidenih 208.650 evrov (oz. 50 %, kar znaša največ 104.325 evrov).



Co-funded by
the European Union



Projekt, financiran v okviru pogodbe o dodelitvi sredstev št. 101249800, podpira Evropski strokovni center za kibernetско varnost.

Nove prijave projektov v letu 2025

Leto 2025 se je za SI-CERT sklenilo s prijavi projektov, ki so jih partnerski konzorciji posredovali v okviru razpisov iz programa Obzorje Evropa – Civilna varnost (grozd 3) za obdobje 2026–2027. Pri teh projektih je med razpisi prevladovala tema »Nova napredna orodja in procesi za operativno kibernetско varnost« (HORIZON-CL3-2025-02-CS-ECCC-02). Pričakovani izid za vse prijavljene projekte pa je, da bodo razvijali tehnologije, orodja in procese, ki krepijo kibernetско varnost z uporabo tehnoloških komponent umetne inteligence, zlasti generativne umetne inteligence, v skladu z ustreznimi političnimi, pravnimi in etičnimi zahtevami EU. Evropski kompetenčni center za kibernetско varnost (ECCC) bo evalvacije prijavljenih projektov dokončal aprila 2026.

UPORABNOST SEZNAMOV SI CERT ZA ZAŠČITO SISTEMOV IN VPOGLED V NJIHOVO RABO

SI CERT je v letu 2024 uvedel tudi sezname, ki organizacijam omogočajo enostavnejšo in bolj avtomatizirano zaščito njihovih informacijskih sistemov. Gre za nov nabor podatkov, ki dopolnjuje obstoječe storitve in predstavlja pomembno nadgradnjo nacionalne kibernetске odpornosti. Seznami vključujejo potrebne lažne spletne strani, domene, ki se pojavljajo v zavajajočih ali škodljivih kampanjah, ter zgoščene vrednosti škodljive programske opreme. Ker temeljijo na primerih, ki jih je SI CERT obravnaval v okviru svojega dela, odražajo grožnje, ki so dejansko prisotne v slovenskem prostoru.

Posebna prednost novih seznamov je, da so pripravljeni kot referenčne liste, kar organizacijam omogoča neposredno vključevanje v njihove varnostne rešitve, zlasti v sisteme za zaznavanje in obravnavo varnostnih dogodkov (SIEM). Takšna oblika močno poenostavi integracijo, saj podatkov ni treba dodatno obdelovati ali prilagajati. Organizacije tako lahko hitreje vzpostavijo avtomatizirane postopke za prepoznavanje in blokiranje zlonamernega prometa, kar je ključno v okolju, kjer se grožnje pojavljajo in spreminjajo izjemno hitro.

Uporaba seznamov se je v kratkem času izkazala za zelo učinkovito.

Seznami domen so prav tako dobro sprejeti, saj jih številne organizacije vključujejo v svoje strežnike DNS, kar omogoča blokiranje zlonamernih domen že na ravni omrežja. Pomembno je tudi, da so domenski seznami SI-CERT vključeni med vire škodljivih domen pri ponudnikih rešitev DNS, kot sta Quad9 in DNS4EU, kar dodatno povečuje njihov doseg in uporabnost.

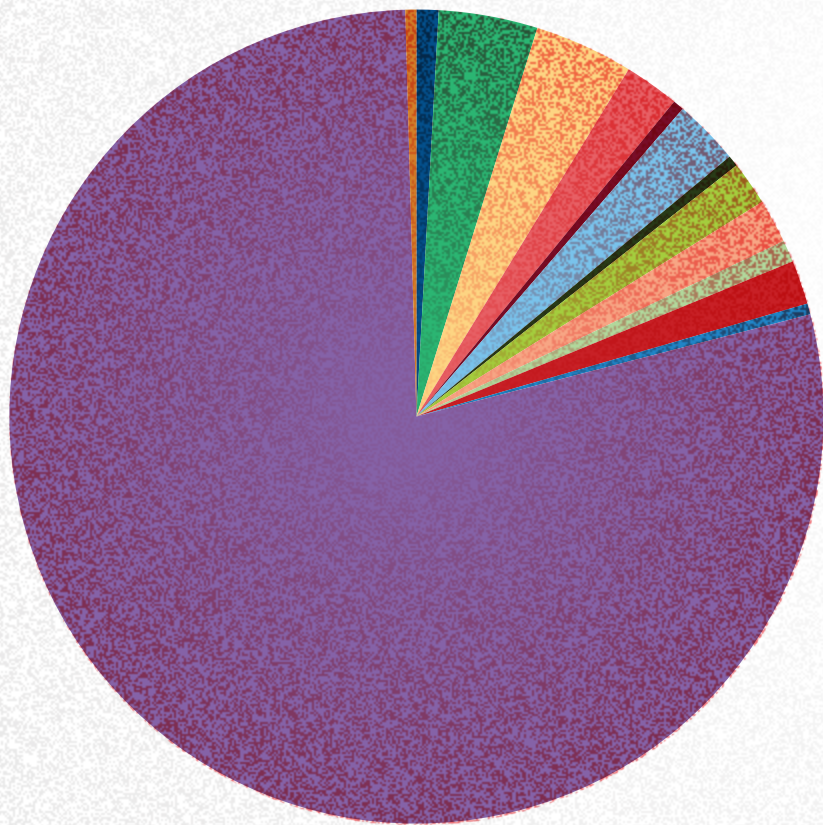
Del novega niza storitev je tudi MISP feed, ki vsebuje dogodke, ki jih je SI CERT objavil in so namenjeni širši javnosti. Feed organizacijam omogoča, da te podatke enostavno vključijo v svoje sisteme, kar dodatno podpira avtomatizacijo in usklajenost obrambnih mehanizmov.

Največ zanimanja je za sezname potrjenih lažnih spletnih strani, ki jih organizacije vključujejo v filtre elektronske pošte in spletnega prometa, s čimer zmanjšujejo tveganje uspešnih prevar.

SI CERT s tem ohranja vlogo osrednjega nacionalnega vira informacij o kibernetških grožnjah.

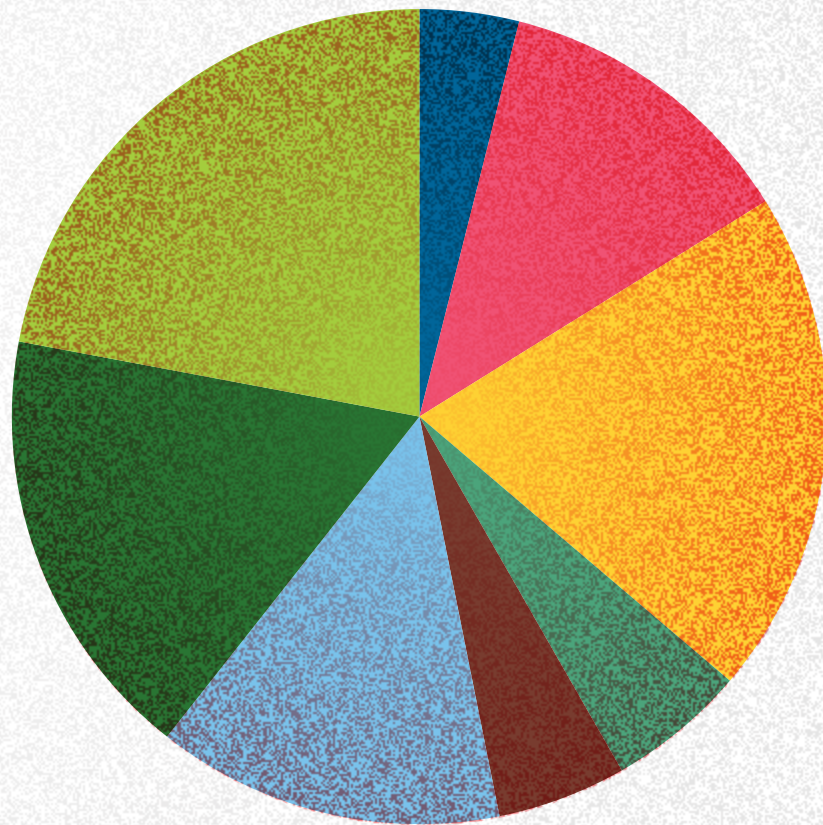
Uvedba seznamov je pomemben korak k večji operativni pripravljenosti slovenskega kibernetškega prostora. Organizacijam omogoča hitrejšo in bolj usklajeno odzivanje na grožnje, zmanjšuje izpostavljenost najpogostejšim oblikam zlorab in krepi odpornost celotnega ekosistema. Dejstvo, da so sezname v kratkem času postali del vsakodnevnih postopkov zaščite številnih organizacij, potrjuje njihovo uporabnost in pomembno vlogo pri zagotavljanju kibernetške varnosti v Sloveniji.

SI	180
PT	1
CY	2
CZ	9
DE	9
EU	5
FR	1
GB	6
HK	1
HR	4
IE	4
IN	2
NL	4
US	1



Statistika zahtev po seznamih s spletnega strežnika glede na državo

/misp/feed/manifest.json	10
/misp/rpz/all.txt	31
/misp/rpz/last.txt	51
/misp/sha1/list.txt	14
/misp/sha256/all.txt	13
/misp/sha256/list.txt	35
/misp/urls/all.txt	44
/misp/urls/last.txt	56



Statistika zahtev po seznamih s spletnega strežnika glede na tip seznama

V LETU 2025

Dodanih

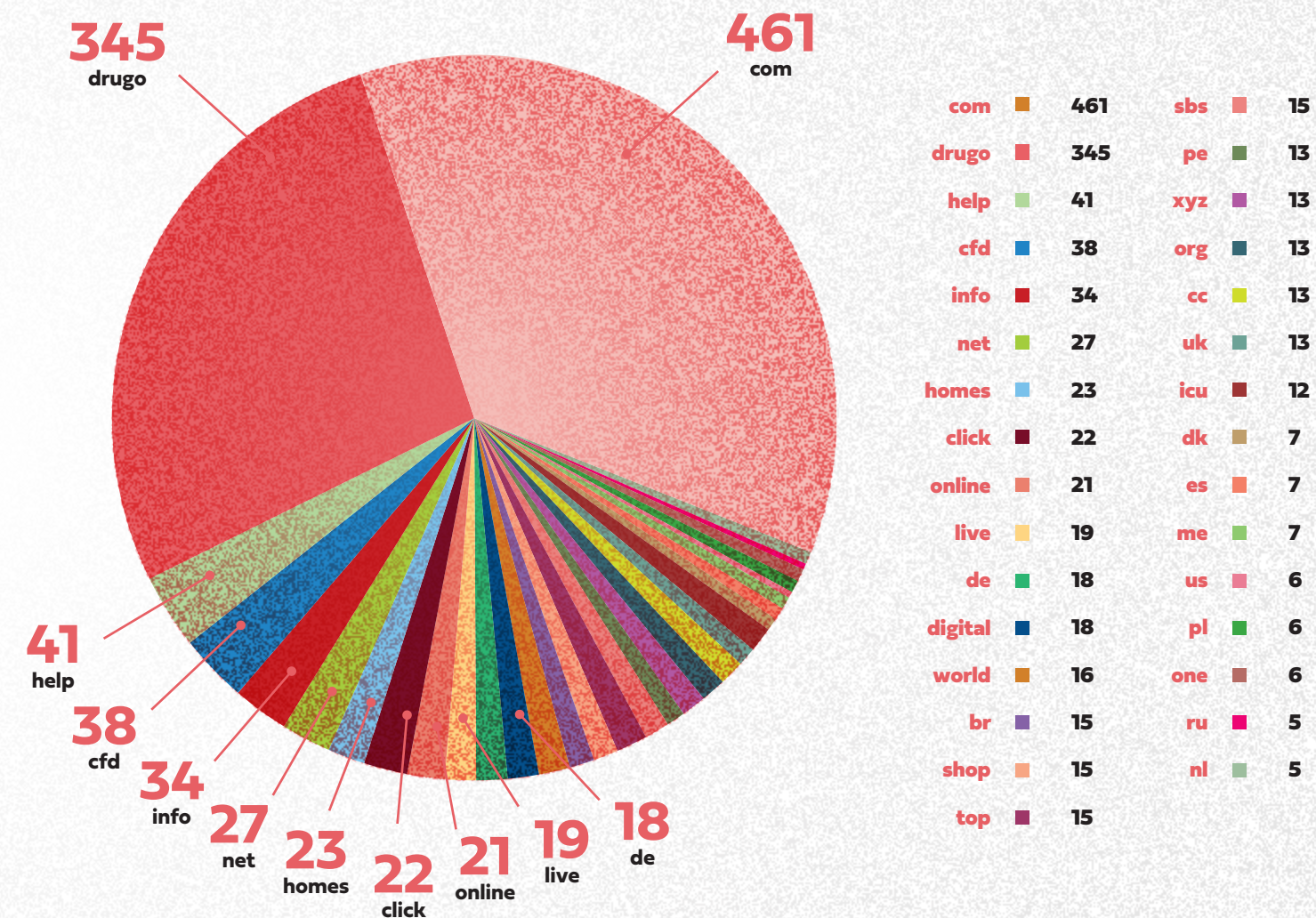
1438

dogodkov MISP, ki jih je prispeval SI-CERT.

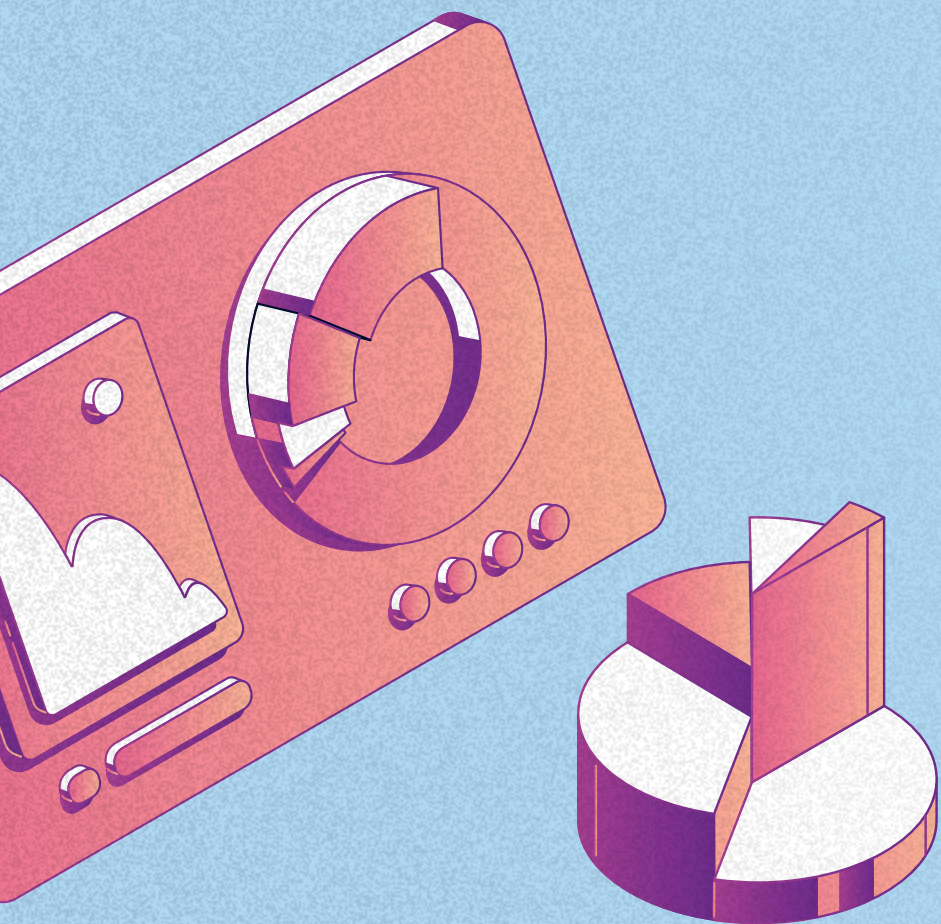
Od tega je več kot

1000

dogodkov namenjenih zaščiti širšega slovenskega kibernetkega prostora.



10 najbolj pogostih vrhnjih domen na phishing seznamu SI-CERT v letu 2025



VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALCI

Leta 2022 je SI-CERT uvedel prvolinijsko podporo za obravnavo tehnično manj zahtevnih incidentov. Namen vpeljave linije je optimizacija postopkov, ki bodo skrajšali čas obdelave podatkov in izvedbe potrebnih ukrepov.

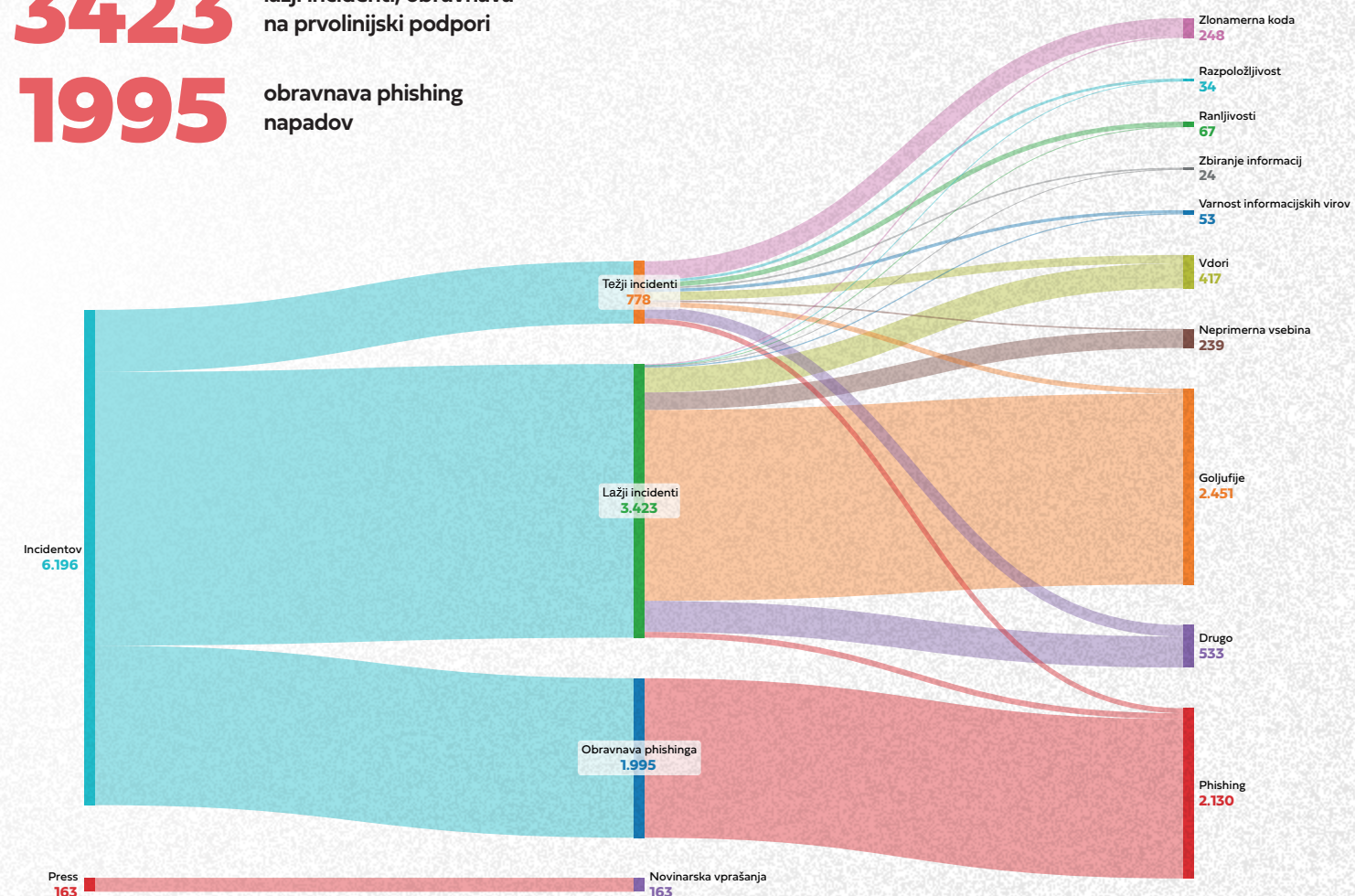
V letu 2025 je SI-CERT obravnaval 6196 incidentov in jih peljal skozi tri različne postopke:

778 tehnično zahtevnejši incidenti

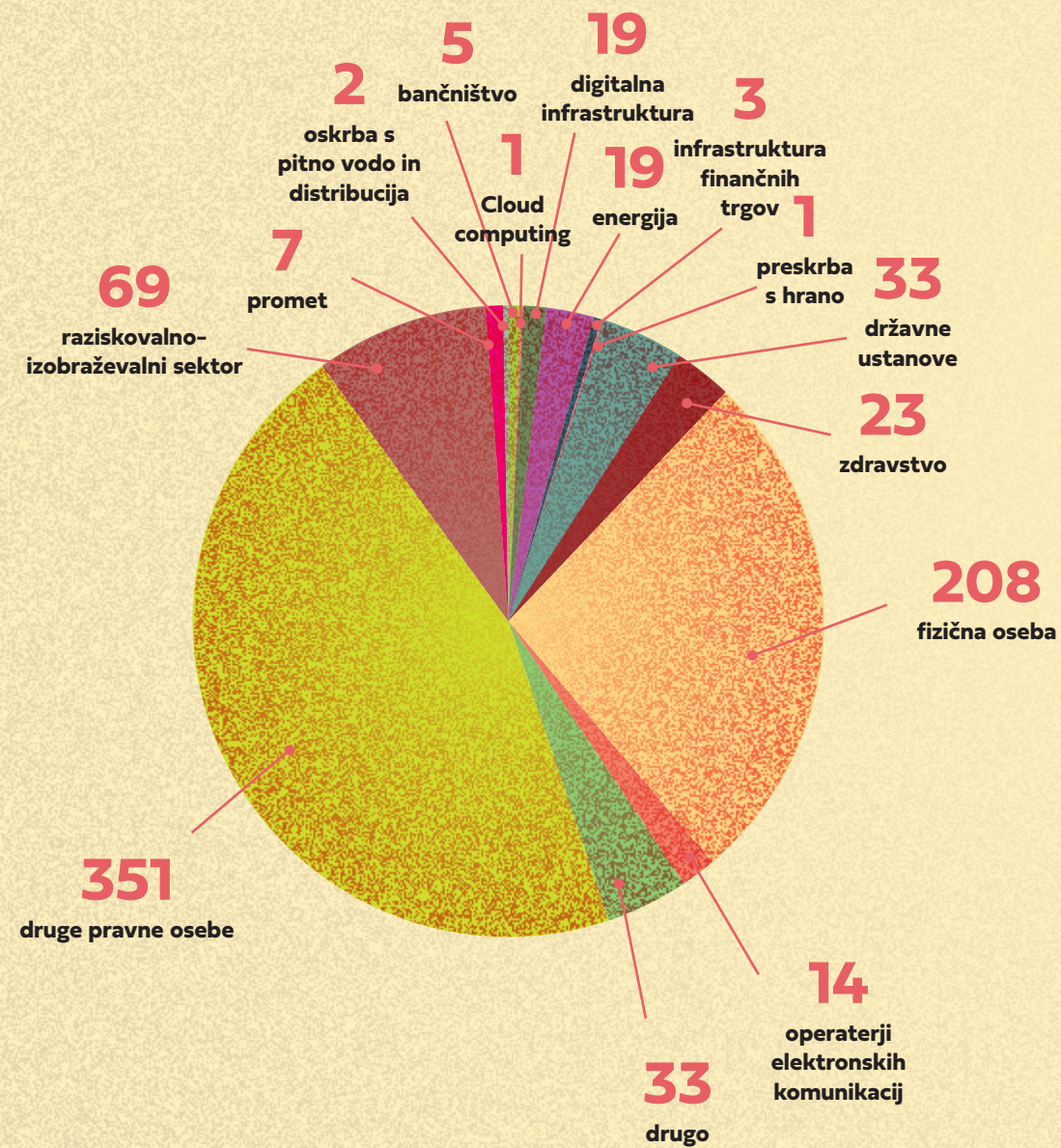
3423 lažji incidenti, obravnava na prvolinijski podpori

1995 obravnava phishing napadov

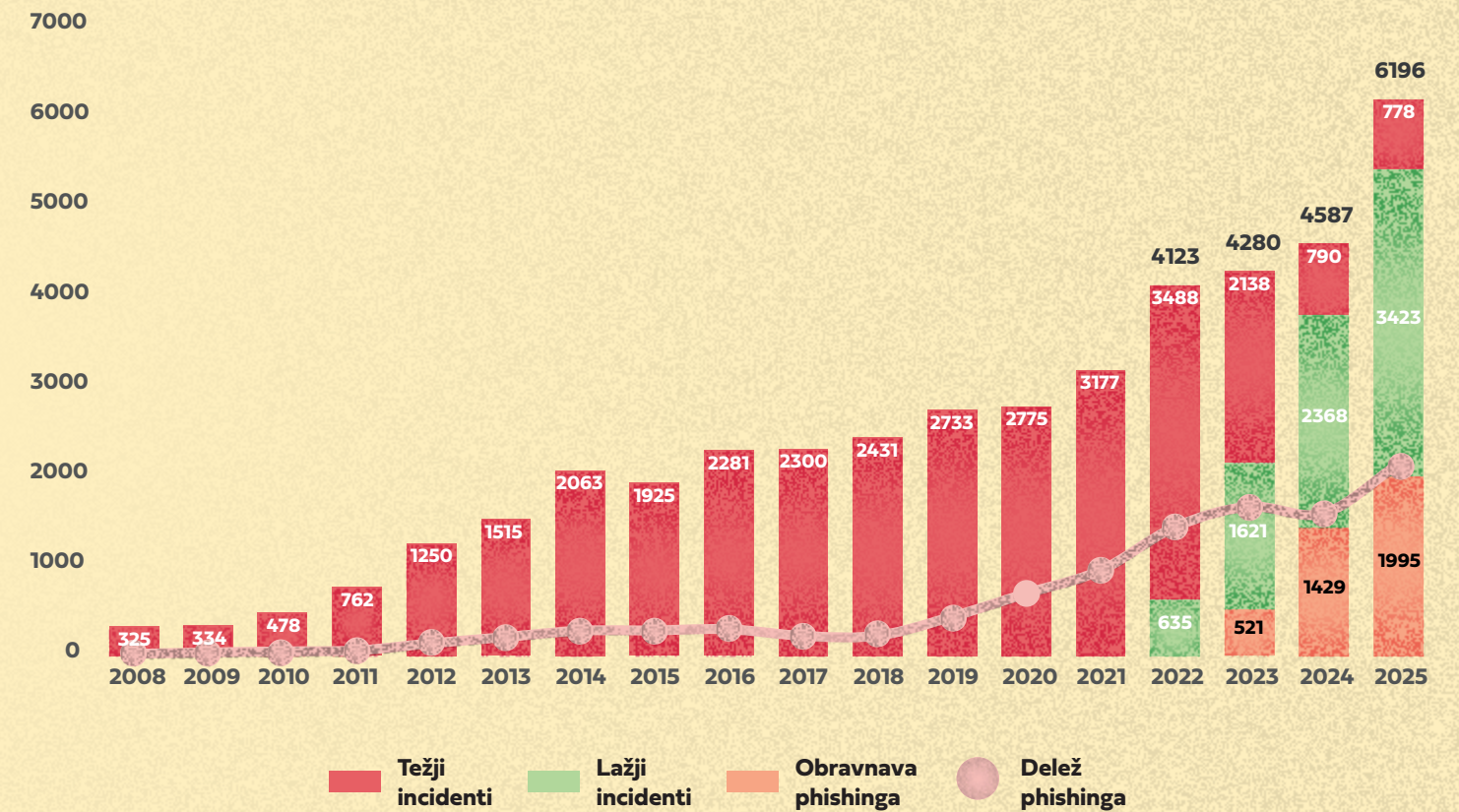
Ob uvedbi različnih linij obravnave prihaja tudi do odstopanj zaradi primerov, ki ostanejo nerazvrščeni v spodaj prikazane kategorije incidentov, to pa običajno zahteva ročni pregled in dopolnjevanje podatkov.



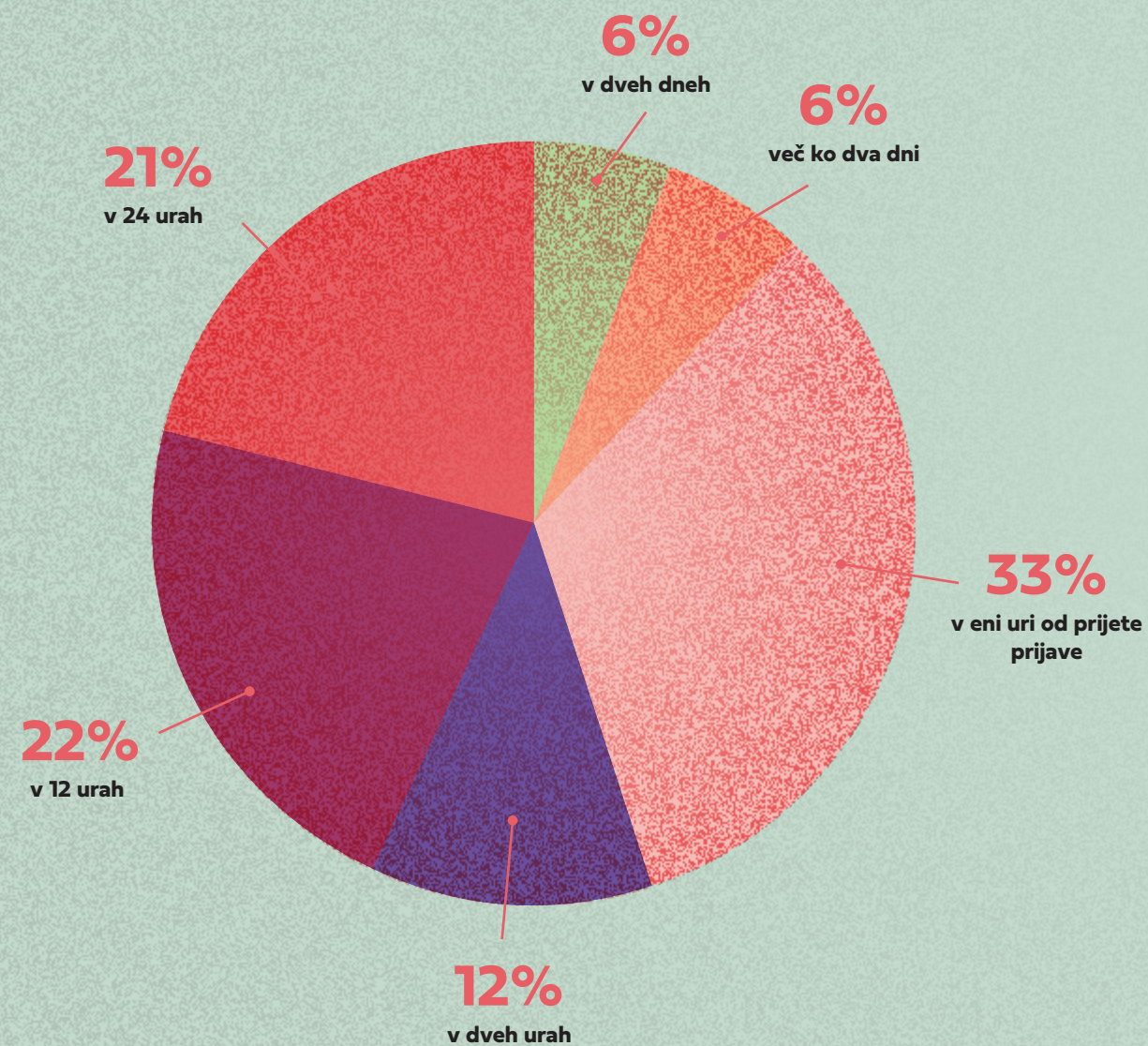
PRIJAVITELJI PO SEKTORJIH



INCIDENTI SKOZI LETA



ODZIVNI ČAS SI-CERT



4337

prijav

1424 v eni uri od prijete prijave

510 v dveh urah

981 v 12 urah

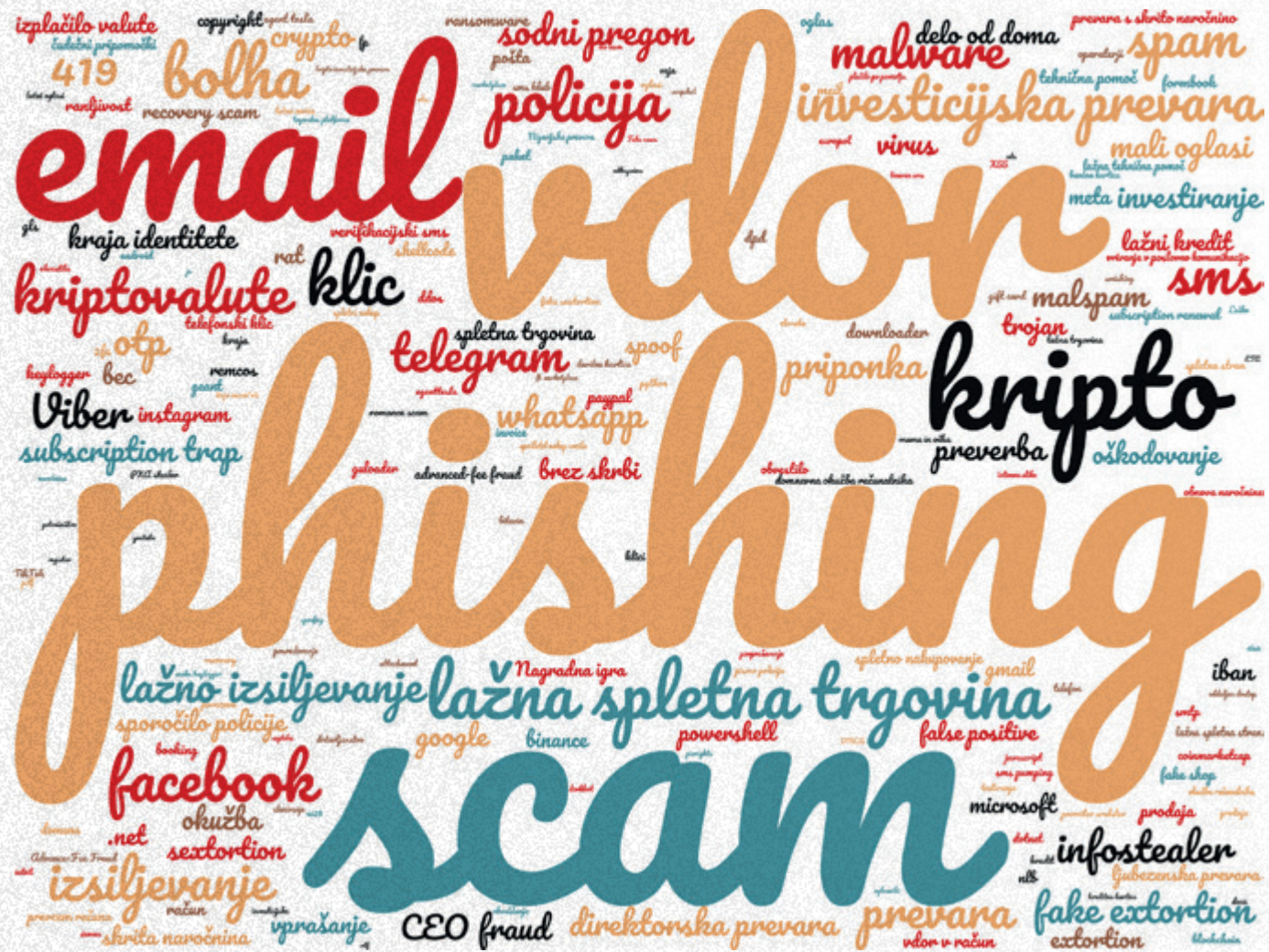
902 v 24 urah

275 v dveh dneh

245 več kot dva dni

Upoštevane so samo prijave, razvrščene v liniji težjih in lažjih incidentov.

V OBRAVNAVANIH INCIDENTIH



Skupina	Vrsta incidenta	2022	2023	2024	2025
Neprimerna vsebina	Neželena sporočila	97	92	149	214
	Žaljiva vsebina	9	7	22	20
	Nasilna vsebina	1	0	2	5
Zlonamerna koda	Virus	8	9	13	17
	Črv	0	2	0	4
	Trojanski konj	278	140	110	168
	Vohunska programska oprema	2	1	0	0
	Dialler	0	1	0	0
	Rootkit	0	1	1	0
	Boti in botneti	8	4	8	2
	Nadzorni strežnik	1	0	0	1
	Izsiljevalski virus	45	32	25	29
	Orodje za oddaljen nadzor (RAT)	33	22	26	27
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	42	22	24	20
	Prestrezanje komunikacije	0	1	0	1
	Socialni inženiring	3	0	2	3
Poskusi vdora	Izkoriščanje znane ranljivosti	3	5	0	4
	Poskusi prijav, bruteforce in napadi s slovarjem	18	24	14	9
	Nova vrsta napada	0	0	0	0
Vdori	Zloraba privilegiranega uporabniškega računa	0	3	12	8
	Zloraba nepriviligiranega uporabniškega računa	112	150	212	378
	Napad na aplikacijo	6	11	19	19
Razpoložljivost	Napad onemogočanja	5	5	8	2
	Porazdeljen napad onemogočanja	17	21	55	19
	Sabotaža	0	1	0	0
	Izpad delovanja naprav ali omrežja	1	7	6	13
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	8	4	14	20
	Nepooblaščno spreminjanje podatkov	15	18	19	24
	Odtekanje informacij	5	5	5	9
Goljufije	Nepooblaščno izkoriščanje virov	6	13	42	55
	Intelektualna lastnina in avtorske pravice	12	2	20	16
	Kraja identitete	48	65	64	62
	Phishing sporočilo	1221	1610	1451	2104
	Phishing spletno mesto	211	47	44	26
	Spletno nakupovanje	113	286	239	393
	Goljufija z vnaprejšnjim plačilom	181	177	108	105
	Izsiljevanje	346	329	342	386
	Druge goljufije	762	760	973	1533
Ranljivosti	Odgovorno razkrivanje	4	9	8	19
	Razkritje ranljivosti	53	20	18	16
	Ranljivi sistemi in naprave	15	13	23	32
Drugo	Drugo	320	347	418	404
	Novinarsko vprašanje	1	0	1	1
Test	Namenjeno preizkusom	1	2	2	2
Skupaj		4011	4268	4499	6170
Nerazvrščenih		112	12	0	26
Vseh incidentov		4123	4280	4499	6196

VIŠINA OŠKODOVANJ V LETU 2025

Na SI-CERT lahko prijavitelj ob priglašnem incidentu tudi navede višino oškodovanja, vendar je to prostovoljno, zato imamo le delni vpogled v oškodovanja. Vseeno pa je to koristno za spremljanje najbolj aktualnih goljufij in pripadajočih višin oškodovanj:

- 260.000 €

najvišje oškodovanje v krypto prevari
- 170.000 €

najvišje oškodovanje pri vrivanju v poslovno komunikacijo (angl. Business E-mail Compromise)
- 46.000 €

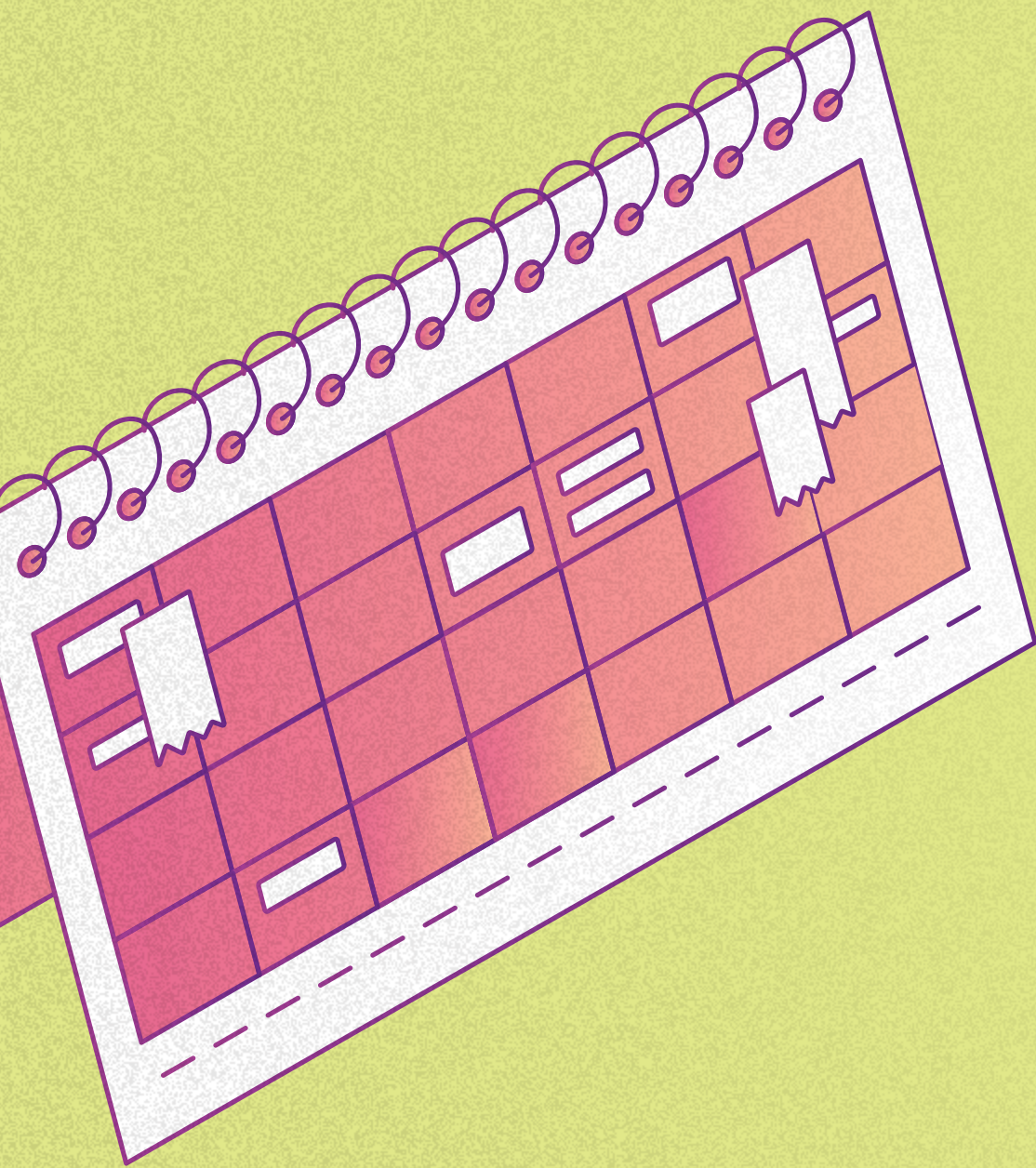
povprečno oškodovanje v phishing napadu
- 17.000 €

povprečno oškodovanje v ljubezenski prevari

PODATKI SLOVENSKE POLICIJE ZA LETO 2025



Vrsta golufije	Število kaznivih dejanj	Škoda v EUR
investicijska vlaganja	1037	25.420.000
BEC/ CEO	68	5.733.000
e-banke	122	5.043.000
romantična prevara	56	1.639.000
nikoli dostavljen artikel	646	1.600.000
nigerijska prevara	17	160.000
sklenitev pogodbe	121	383.000
sorodnik v težavah	10	22.000
pridobitev kredita	41	176.000
zloraba plačilne kartice	431	445.000



IZPOSTAVLJENE TEME V LETU 2025

30 LET POMOČI, ZAUPANJA IN GRAJENJA KIBERNETSKE SKUPNOSTI

Nacionalni odzivni center za kibernetsko varnost SI-CERT je v letu 2025 praznoval 30 let delovanja.

Začetek delovanja sega v jesen leta 1995, ko je SI-CERT s Švedskega kraljevega inštituta za tehnologijo KTH prejel prvo prijavo kibernetskega incidenta. Takrat si verjetno nihče ni predstavljal, kako močno bo digitalizacija v naslednjih desetletjih prežela naša življenja. Temu primerno so tudi posledice kibernetskega incidenta danes lahko veliko resnejše.

Danes, po treh desetletjih delovanja, ostaja SI-CERT osrednja točka za odzivanje na kibernetske grožnje v Sloveniji. Naše poslanstvo je oblikovanje zavedanja o trenutnem stanju v kibernetskem prostoru in vzdrževanje strokovnega znanja na področjih digitalne forenzike, analize zlonamerne kode in postopkov odzivanja na kibernetske grožnje ter incidente. Vodja SI-CERT Gorazd Božič poudarja: *»Odzivni center SI-CERT je danes dobro vpet v mednarodno skupnost in v javnosti prepoznan kot strokovno podkovan in zaupanja vreden partner. Naš program 'Varni na internetu' je velikokrat vzor drugim v EU kot učinkovito in usmerjeno ozaveščanje na področju varne uporabe interneta.«*

30-letnico delovanja je SI-CERT obeležil z odprtjem razstave »Hekerji – kibernetska (ne)varnost« v Računalniškem muzeju v Ljubljani. Razstava je obiskovalcem omogočila interaktivni vpogled v zgodbe iz zakulisja hekerske kulture, od prvih spletnih incidentov v Sloveniji do sodobnih kibernetskih groženj, in prikazala razvoj kibernetske varnosti skozi tri desetletja. Poudarila je pomen zavedanja o kibernetski varnosti, kritičnega razmišljanja, zaščite zasebnosti in etičnega ravnanja v digitalnem okolju. Razstava je bila odprta do junija 2026 in je obiskovalcem omogočala neposreden stik s temami, ki jih običajno poznamo le iz naslovov novic.



**Ekipa SI-CERT ob odprtju razstave
»Hekerji – kibernetska (ne)varnost«**

Nagrada za življenjsko delo ob 30. obletnici SI-CERT

Na konferenci INFOSEK, osrednjem in največjem dogodku za informacijsko varnost v Sloveniji, vsako leto podelijo priznanja za prispevek k razvoju področja kibernetске varnosti. Nacionalnemu odzivnemu centru za kibernetско varnost SI-CERT je bila ob 30. obletnici delovanja podeljena **nagrada za življenjsko delo na področju informacijske varnosti**. Tradicionalna priznanja za izstopajoče dosežke na področju kibernetске varnosti sta poleg SI-CERT prejela tudi stanovska kolega iz podjetij Petrol in Telekom Slovenije.



Nagrado je v imenu SI-CERT prevzel namestnik vodje Tadej Hren, ki je ob priložnosti poudaril: **»Nagrada za življenjsko delo na področju informacijske varnosti nam izredno veliko pomeni. SI-CERT letos obeležuje 30-letnico delovanja. Začeli smo v času, ko se o informacijski varnosti praktično ni govorilo, danes pa digitalizacija prežema naša življenja, posledice kibernetskega incidenta pa so veliko resnejše kot v času modemov in IRC-a. V tem okolju smo s premagovanjem mnogih ovir tudi mi rasli in se strokovno krepili, zato lahko danes primerno obvladujemo sodobne kibernetске grožnje. Izzivov v prihodnosti nam ne bo zmanjkalo.«**

Ljubljana FIRST Technical Colloquium 2025

SI-CERT je v sodelovanju s svetovnim združenjem odzivnih in varnostnih centrov FIRST ter z Registrom za vrhno domeno .si 9. in 10. decembra 2025 izvedel mednarodni tehnični kolokvij o kibernetски varnosti. Tehnični kolokvij je namenjen predvsem članom združenja FIRST, ker pa **gre za edinstveno možnost tovrstnega izobraževanja, je SI-CERT s povabilom omogočil udeležbo tudi slovenskim podjetjem in državnim organom**, ki imajo pomembno operativno vlogo pri krepitvi kibernetске varnosti v Sloveniji.



Na dogodku je bilo v ospredju tehnično usposabljanje; kolokvij je vključeval tudi predstavitve uveljavljenih strokovnjakov in dve praktični delavnici. Na zaključni dan dogodka, 11. decembra, je potekalo še zaprto srečanje skupin odzivnih centrov regij Zahodnega Balkana. Srečanje je bilo namenjeno krepitvi kapacitet in operativnega sodelovanja mladih nacionalnih odzivnih centrov v teh regijah. SI-CERT že vrsto let aktivno podpira ustanavljanje odzivnih centrov in izboljšanje njihovega povezovanja v regiji.



Posvet o izobraževanju zaposlenih o kibernetски varnosti – novi pristopi za nove grožnje

Ena od pomembnih dejavnosti odzivnih centrov je tudi prenos znanja. V ta namen je SI-CERT 4. junija 2025 v Ljubljani organiziral dogodek, s katerim so želeli poudariti pomen izobraževanja zaposlenih. Dogodek je pod naslovom **»Novi pristopi za nove grožnje«** združil strokovnjake s področja kibernetске varnosti, kadrovskih služb ter izobraževanja. Namen posveta je bil izmenjati dobre prakse, predstaviti učinkovite pristope k izobraževanju zaposlenih ter razpravljati o vlogi človeškega dejavnika pri grajenju varnostne kulture v organizacijah.

Dogodek je izpostavil pogosto zmotno predstavo, da je za varnost odgovoren zgolj IT-oddelek. V resnici je kibernetսка varnost danes temeljna komponenta digitalne pismenosti, ki se tiče vseh – od tajništva do vodstva.

Srečanje je odprlo razpravo o tem, kako človeški dejavnik vpliva na varnostne incidente in katere metode izobraževanja so najučinkovitejše za povečanje ozaveščenosti zaposlenih. Udeleženci so predstavili primere dobrih praks iz slovenskih in mednarodnih organizacij, vključno z inovativnimi oblikami usposabljanja in pristopi za spodbujanje sodelovanja zaposlenih pri preprečevanju kibernetских groženj. Dogodek je omogočil tudi izmenjavo izkušenj ter konkretnih priporočil, kako izboljšati varnostno vedenje v različnih vrstah organizacij.

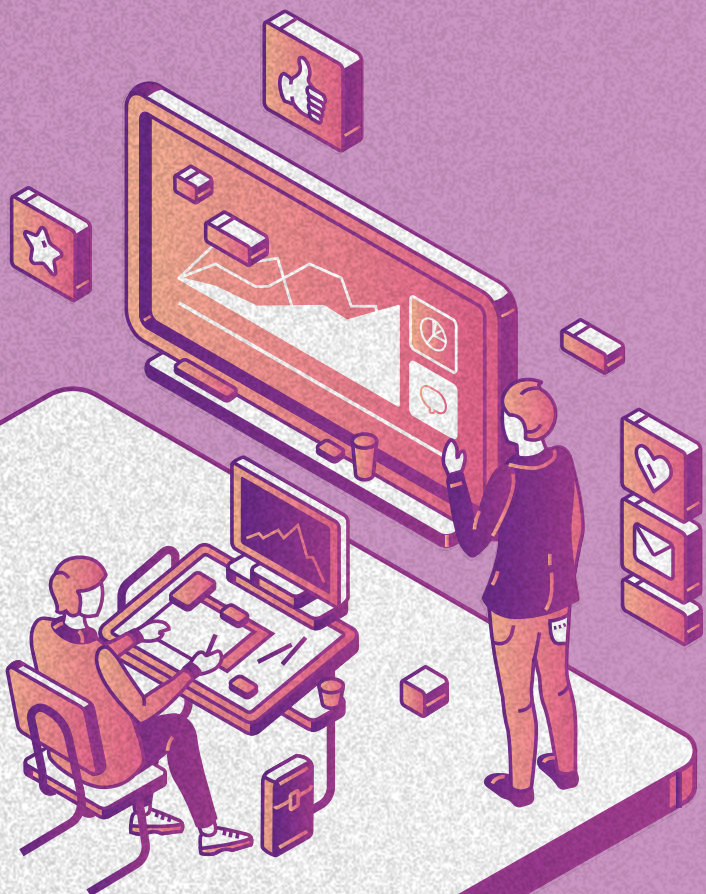


Serija izobraževalnih spletnih seminarjev

SI-CERT je v letu 2025 izvedel serijo šestih spletnih seminarjev, s katerimi je naslovil konkretne kibernetске incidente in grožnje, ki slovenskim podjetjem in posameznikom predstavljajo izziv. Spletni seminarji na Zoomu so bili uspešno in tehnično brezhibno izvedeni, skupaj so pritegnili 1874 udeležencev v živo, posnetki seminarjev pa so imeli več kot 6000 ogledov.

- Spletni seminarji so se ukvarjali z različnimi tematikami:
- **Kibernetսка varnost za spletne trgovce in vzdrževalce spletnih strani;**
 - **Zlorabe v svetu kriptovalut;**
 - **Napredni kibernetски napadi na podjetja;**
 - **Priglasitev kibernetских incidentov;**
 - **Infostealerji pod drobnogledom;**
 - **Zlonamerna koda slovenskega kibernetskega kriminala.**

Na voljo so **posnetki vseh spletnih seminarjev**, saj verjamemo, da lahko pomagajo pooblaščenim osebam za varstvo podatkov, odgovornim za skladnost, vodjem informacijske in korporativne varnosti ter vsem, ki se v organizaciji srečujejo z obravnavo kibernetских incidentov.



NACIONALNI PROGRAM OZAVEŠČANJA O KIBERNETSKI VARNOSTI



VARNI NA INTERNETU

Od mene je odvisno vse.

Nacionalni program ozaveščanja »Varni na internetu« smo v SI-CERT zasnovali z namenom izobraževanja širše slovenske javnosti o varni uporabi interneta in prepoznavanja spletnih tveganj. Naše delo temelji predvsem na preventivnem delovanju – opozarjanju in izobraževanju spletnih uporabnikov, kako prepoznati različne oblike spletnih goljufij.

Program izvajamo že od leta 2010 in naslavljamo precej široko področje problematike informacijske varnosti. Leta 2025 je bil sprejet nov Zakon o informacijski varnosti (ZInfV-1), ki jasno definira naloge odzivnega centra SI-CERT in ob bok drugim dejavnostim postavlja tudi ozaveščanje uporabnikov na področju informacijske varnosti. Zakonsko predpisane naloge izvajanja programov ozaveščanja, opredeljene v 9. odstavku 15. člena ZInfV-1, SI-CERT izpolnjuje skozi številne komunikacijske in medijske dejavnosti programa »Varni na internetu«.

Program »Varni na internetu« je namenjen najširši slovenski javnosti, poseben sklop vsebin pa namenjamo malim podjetjem, obrtnikom in samostojnim podjetnikom. Kot glavni cilj programa je opredeljeno **opolnomočenje spletnih uporabnikov, da bodo znali prepoznati različna spletna tveganja in nevarnosti ter ustrezno zaščititi svoje naprave in uporabniške račune.**

Program »Varni na internetu« je namenjen najširši slovenski javnosti, poseben sklop vsebin pa namenjamo malim podjetjem, obrtnikom in samostojnim podjetnikom. Kot glavni cilj programa je opredeljeno opolnomočenje spletnih uporabnikov, da bodo znali prepoznati različna spletna tveganja in nevarnosti ter ustrezno zaščititi svoje naprave in uporabniške račune.

Program pokriva ključne problematike: okužbe z zlonamerno kodo, vdore v uporabniške račune, lažne spletne trgovine, različne oblike spletnih goljufij, phishing kraje podatkov. Zaupanje v programske rešitve pred takimi zlorabami ne obvaruje – edina rešitev je kontinuirano izobraževanje spletnih uporabnikov.

- Program nagovarja odrasle 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 upokoјenci, delovno neaktivni prebivalci, ki niso več vpeti v formalne procese izobraževanja, hkrati pa niso deležni dodatnih izobraževanj o kibernetiki varnosti.
- Zaposleni, samozaposleni, manjša podjetja: druga ciljna skupina so **zaposleni v manjših podjetjih**, vodstva manjših podjetij in IT-kader, saj potrebujejo bolj specifične napotke in priporočila, hkrati pa imajo omejene vire.

Vse dejavnosti programa ozaveščanja »Varni na internetu« so v celoti financirane s sredstvi Urada Vlade Republike Slovenije za informacijsko varnost.



Rekordni dosežek za spletni tečaj »Varni v pisarni«

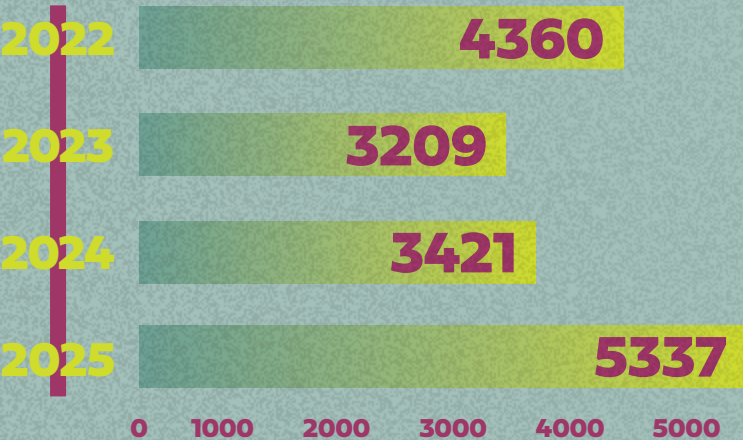
SI-CERT je leta 2021 zasnoval brezplačni spletni tečaj o osnovah informacijske varnosti za zaposlene »Varni v pisarni«. Spletni tečaj na zelo enostaven, razumljiv in vizualno privlačen način zaposlenim v manjših podjetjih predstavi osnove informacijske varnosti.

V letu 2025 je SI-CERT zabeležil rekordno število prijav novih tečajnikov, ki so uspešno opravili spletni tečaj, in sicer kar 5337 novih registriranih uporabnikov.

Eden od razlogov za porast zanimanja za spletni tečaj SI-CERT je tudi sprejetje novega Zakona o informacijski varnosti, ki zavezancem iz zakona predpisuje izvajanje rednih usposabljanj za ozaveščanje zaposlenih. URSIV je izdal priporočene vsebine za osnovno usposabljanje s področja informacijske in kibernetske varnosti, ki med drugim vključujejo tudi izvedbo usposabljanj zaposlenih glede na različne vloge v podjetju, izdajo in hrambo potrdil o udeležbi ter obravnavajo vsebine in problematike, ki jih obravnava tudi tečaj »Varni v pisarni«.

Na SI-CERT lahko brez zadržkov zatrdimo, da spletni tečaj »Varni na internetu« ustreza vsem zahtevam glede izobraževanja zaposlenih, kot jih URSIV priporoča zavezancem, in v prihodnjih letih pričakujemo nadaljnjo rast števila tečajnikov.

Spletni tečaj Varni v pisarni



5.337
novih tečajnikov

17.600
vseh tečajnikov



Kampanja ob mesecu kibervarnosti »Meni se to ne more zgoditi!«

»Meni se to ne more zgoditi!« je stavek, ki ga na SI-CERT pogosto slišimo. Veliko uporabnikov interneta verjame, da so pred spletnimi prevarami varni. Na SI-CERT že tri desetletja spremljamo dogajanje na področju kibernetskih groženj in vidimo, da je resničnost povsem drugačna – žrtev spletne prevare lahko postane vsakdo. Ravno na to dejstvo smo opozorili ob evropskem mesecu kibervarnosti 2025 in v okviru programa »Varni na internetu« izvedli nacionalno ozaveščevalno kampanjo, katere cilj je bil opozoriti, da spletne prevare predstavljajo resno grožnjo za vse spletne uporabnike. Kampanja je temeljila na aktualnih podatkih SI-CERT, ki kažejo na porast phishing prevar, investicijskih goljufij in lažnih spletnih trgovin. Jedro kampanje so predstavljale štiri video zgodbe, povzete po resničnih primerih slovenskih uporabnikov, ki pokažejo, da se prevara lahko zgodi komurkoli.

Poseben poudarek kampanje sta predstavljali gverilski akciji z interaktivnimi inštalacijami v urbanem prostoru, ki sta mimoidoče nagovarjali, naj prisluhnejo izpovedim žrtev spletnih prevar. To niso oddaljene zgodbe iz tujine – to so lahko naši sosede, naši prijatelji. Ob začetku kampanje so bile inštalacije postavljene v Ljubljani, sredi oktobra pa še v Mariboru. Mimoidoče so spodbujale, da »pokukajo skozi okno« oziroma v pogovorno okno ter prisluhnejo resničnim zgodbam o spletnih prevarah, s čimer je kampanja neposredno nagovorila javnost v vsakdanjem okolju.



Oglaševanje je potekalo na digitalnih platformah Meta in Google ter se iz oktobra razširilo tudi v november 2025. Izbor kanalov je bil prilagojen doseganju odraslih spletnih uporabnikov, ki uporabljajo spletno in mobilno bančništvo, nakupujejo na spletu ter uporabljajo družbena omrežja. Kampanja je požela tudi veliko medijske pozornosti.

'Meni se to ne more zgoditi': na Tinderju spoznal punco in izgubil vse prihranke

Ljubljana, 01. 10. 2025 12:35 • 2 min branja • 115



Veliko spletnih uporabnikov verjame, da ne bodo nikoli nasedli spletnim prevaram, a statistika kaže, da število prijav in višina finančne škode v Sloveniji iz leta v leto naraščata. Nacionalni odzivni center za kibernetsko varnost SI-CERT opozarja, da lahko žrtev postane vsak. Maja, Teo, Gaja in Marjan – štiri zgodbe, povzete po resničnih primerih.

Posnetek zaslona prispevka, objavljenega na portalu 24ur.com



Inštalacija, pripravljena v okviru evropskega meseca kibervarnosti (foto: Damjan Žibert, 24ur.com)

Sklop radijskih oddaj
o spletnih prevarah
– Prvi program Radia Slovenija

V letu 2025 je SI CERT skupaj s Prvim programom Radia Slovenija pripravil serijo 18 radijskih oddaj na temo spletnih prevar in kibernetске varnosti, ki so bile predvajane v okviru podkasta **Aktualna tema**.

Vsaka oddaja je obravnavala različne vidike spletnih prevar – od lažnih telefonskih klicev in prevare z vrivanjem v komunikacijo do psiholoških dejavnikov, ki pripeljejo uporabnike do tega, da nasedejo napadalcem. Oddaje so strokovno osvetlile pogoste trike spletnih goljufov, pomen prepoznavanja opozorilnih znakov in praktične nasvete za boljšo zaščito pred spletnimi prevarami ter tako prispevale k ozaveščanju javnosti o aktualnih kibernetских grožnjah.

Druge aktivnosti programa
Varni na internetu

Priročnik ABC varnosti na spletu

V letu 2025 je bilo natisnjenih in razposlanih 3000 izvodov priročnika **ABC varnosti na spletu**, ki je primarno namenjen starejšim in manj večim uporabnikom spleta, kot usmeritev in pomoč pa tudi izvajalcem računalniških usposabljanj po Sloveniji. Med večjimi partnerji pri diseminaciji priročnikov so Simbioza, socialno podjetje Citilab ter številne univerze za tretje življenjsko obdobje po Sloveniji.

Izzivi na družbenih omrežjih

Pomemben del ozaveščanja je tudi komunikacija na družbenih omrežjih, kjer praktično vsakodnevno pripravljamo opozorila o novih prevarah in nasvete za spletno varnost. Na Facebook strani »Varni na internetu« imamo že več kot 44.500 sledilcev, na Instagramu pa 6145. Obe strani sta zelo pomembna kanala za deljenje vsebin in doseg ciljnih javnosti. Kljub verodostojnim in koristnim vsebinam pa se program »Varni na internetu« **neprestano srečuje s težavo blokiranja in brisanja vsebin s strani Mete**, bodisi zaradi uporabe ključnih besed, kot so 'kripto', 'phishing', 'prevara', bodisi zaradi nazornih grafičnih prikazov prijav (posnetki zaslona sporočil za krajo podatkov), ki jih Meta, kljub jasni označbi, da gre za ozaveščanje, prepozna kot kršitev.

Naslov publikacije: Poročilo o kibernetски varnosti za leto 2025
Avtor publikacije: Nacionalni odzivni center za kibernetско varnost SI-CERT

Leto izida: 2026

Naklada: 500 izvodov

Založnik: Akademsko in raziskovalno mrežo Slovenije

Oblikovanje in prelom: MONU – design biro

Vsa letna poročila o kibernetски varnosti v Sloveniji, ki jih izdajamo pri centru SI-CERT, so dostopna na naslovu

www.cert.si/letna_porocila/.



SI·CERT

Nacionalni odzivni center
za kibernetško varnost