POROČILO O KIBERNETSKI VARNOSTI

2023

Nacionalni odzivni center
za kibernetsko varnost SI-CERT.

si·cert

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
@sicert

Ozaveščanje javnosti na področju informacijske varnosti
www.varninainternetu.si

varninainternetu
@varninanetu
varninainternetu

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

URSIV

KAZALO

Uvodni nagovor

RANLJIVA DIGITALIZACIJA

Pospešena digitalizacija pomeni med drugim tudi vedno večjo odvisnost od komunikacijske infrastrukture, v večini primerov gre za internet in omrežja mobilne telefonije. Izsiljevalski virusi postajajo vedno večja težava, zato številne države razmišljajo tudi o prepovedi plačevanja odkupnin kriminalnim skupinam.

Nas pa bolj zanima, kako zmanjšati tveganja za nepooblaščene vstope v omrežja. V kompleksnih sistemih se hitro zgodi, da se pozabi na en sam strežnik nekje na omrežju in je to že dovolj za uspešno izvedbo napada. Ali pa je krivec zaposleni, ki je kliknil na zlonamerno priponko. Zato številna podjetja izvajajo phishing preizkuse na svojih zaposlenih, moramo pa si priznati, da potem ni čudno, če zaposleni ne vedo več, ali priponko odpreti ali ne. Lani smo na primer prejeli številne prijave »phishing« napada, v resnici pa je Microsoft obveščal uporabnike o spremenjenih pogojih uporabe storitev. Tretja pot za storilce pa so ranljivosti, ki omogočijo premostitev zaščitnih mehanizmov.

Leta 2018 smo na podlagi Direktive o varnosti omrežij in informacij (direktiva NIS) dobili Zakon o informacijski varnosti. Na podlagi tega so bili določeni zavezanci, ki so morali sprejeti dodatne ukrepe za zaščito svoje digitalne infrastrukture in dobiti obvezo sporočanja pomembnejših incidentov. Od takrat smo dobili še nekaj sprememb, po enakem kopitu pa se je uvedlo poročanje tudi za operaterje elektronskih komunikacij, pozneje pa še za določene upravljavce osebnih podatkov.

Zdaj imamo pred vrati nove uredbe in direktive, med njimi seveda NIS2, ki bo močno razširila obseg zavezancev in SI-CERT naložila dodatne naloge glede obravnave ranljivosti in izvajanja neinvazivnih pregledov omrežij zavezancev. Zato je v postopku sprejemanja tudi nov Zakon o informacijski varnosti. Bistveno vprašanje pa je, ali bomo zaveze zmogli udejanjiti v praksi in pri tem izoblikovali ustrezno vizijo razvoja, da nadomestimo zaostanek, ki se je ustvaril v zadnjih desetih letih.

Gorazd Božič
Vodja SI-CERT

IZSTOPAJOČE ŠTEVILKE 2023

SI-CERT

4.280
obravnavanih incidentov
(**4%** rast v primerjavi z 2022)

več kot
1.600
primerov phishing napadov

na platformi MISP dodanih več kot
35.000
novih dogodkov

okoli
150
kripto-investicijskih prevar

5.158
izdanih certifikatov tečaja Varni v pisarni

162
novinarskih vprašanj

več kot
50
izpeljanih predavanj na različne teme kibernetske varnosti

slovenska policija zabeleži
27,5 milijonov €
škode v različnih spletnih goljufijah

največji porast je **v kategoriji investicijskih prevar**
kar 13 milijonov €
škode

51 primerov **»BEC« prevar** (vrivanje v poslovno komunikacijo), ki slovenskim podjetjem povzročijo za
7,8 milijonov €
škode

2,4 milijona €
škode zaradi nedostavljenih izdelkov pri spletnem nakupovanju
(večinoma lažne spletne trgovine)

800.000 € škode zaradi ljubezenskih prevar in
3,5 milijona €
zaradi **phishing zlorab v elektronskem bančništvu**

REPUBLIKA SLOVENIJA POLICIJA

INFORMACIJSKI POOBLAŠČENEC

Informacijski pooblaščenec prejme
183 uradnih obvestil o kršitvi varnosti
(Data Breach Notification)

IZSTOPAJOČI DOGODKI

Januar

Organi pregona uničijo več kriminalnih združenj, ki so se ukvarjala z investicijskimi prevarami s kriptovalutami. Kljub temu so se investicijske prevare nadaljevale in zaznamovale celotno leto 2023.

Februar

Slovenski uporabniki začnejo prejemati neobičajna SMS-sporočila z verifikacijskimi kodami (OTP) za storitve, ki jih ne uporabljajo. Ni šlo za zlorabo osebnih podatkov, ampak za izkoriščanje ranljivosti sistemov za pošiljanje verifikacijskih kod.

Marec

Zaživi pobuda Ženske v kibernetski varnosti, ki želi podpreti in povezati strokovnjakinje, ki delujejo na raznolikem področju kibernetske varnosti. K pobudi aktivno pristopi tudi SI-CERT.

April

Zaznan je kibernetski napad na Ministrstvo za zunanje in evropske zadeve vrste APT (Advanced persistent threat). Tovrstne napade običajno izvajajo državno podprti napadalci. Lahko trajajo zelo dolgo časa in jih je izredno težko zaznati.

Maj

Za nacionalni program ozaveščanja Varni na internetu prejmemo nagrado Slovenian Grand Security Award v kategoriji za najboljši strokovni prispevek s področja varnosti. Nagrado vsako leto podeljuje Inštitut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti.

Junij

Objavimo polletno poročilo za leto 2023, ki pokaže rast števila prijav za 4,57 % glede na enako obdobje leta 2022. V prvi polovici leta v povprečju vsak teden odgovorimo na 134 prijav. Število phishing incidentov se umiri po rekordnem letu 2022, vendar še vedno predstavlja dobro tretjino vseh obravnavanih incidentov.

Julij

Univerza v Ljubljani doživi vdor v informacijski sistem. Posledice odpravijo v štirih dneh, njihovo poslovanje pa poteka nemoteno.

Avgust

Policija v Mariboru aretira spletne goljufe, ki so izvajali SMS phishing napade na slovenske uporabnike. Število teh napadov je za kratek čas upadlo, proti koncu leta pa se je število spet povečalo.

September

Proruske hektivistične skupine izvedejo DDoS napade na spletne strani Nacionalnih CSIRT skupin v EU. Tarča je tudi spletna stran https://cert.si, ki je zaradi napada za kratek čas nedosegljiva.

Oktober

Začne se Evropski mesec kibervarnosti, vseevropska kampanja ozaveščanja, ki jo s podporo držav članic organizirata Agencija Evropske unije za kibernetsko varnost (ENISA) in Evropska komisija. Slovenijo v mednarodni kampanji zastopa SI-CERT, v središče aktivnosti pa postavimo starejše uporabnike.

November

Zgodi se odmeven ransomware napad na Holding Slovenskih elektrarn, katerega odgovornost prevzame skupina Rhysida. Ob hitrem ukrepanju strokovnih služb HSE je storilcem uspelo zašifrirati le manjši del sistemov in pridobiti dostop do podatkov, ki niso imeli velike vrednosti.

December

Operaterje elektronskih komunikacij začnemo tedensko obveščati o okuženih sistemih njihovih uporabnikov. Podatke nam pošljejo partnerske organizacije, ki z različnimi metodami pridobijo podatke o okuženih sistemih in jih posredujejo nacionalnim odzivnim centrom po različnih državah.

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.

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. 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:

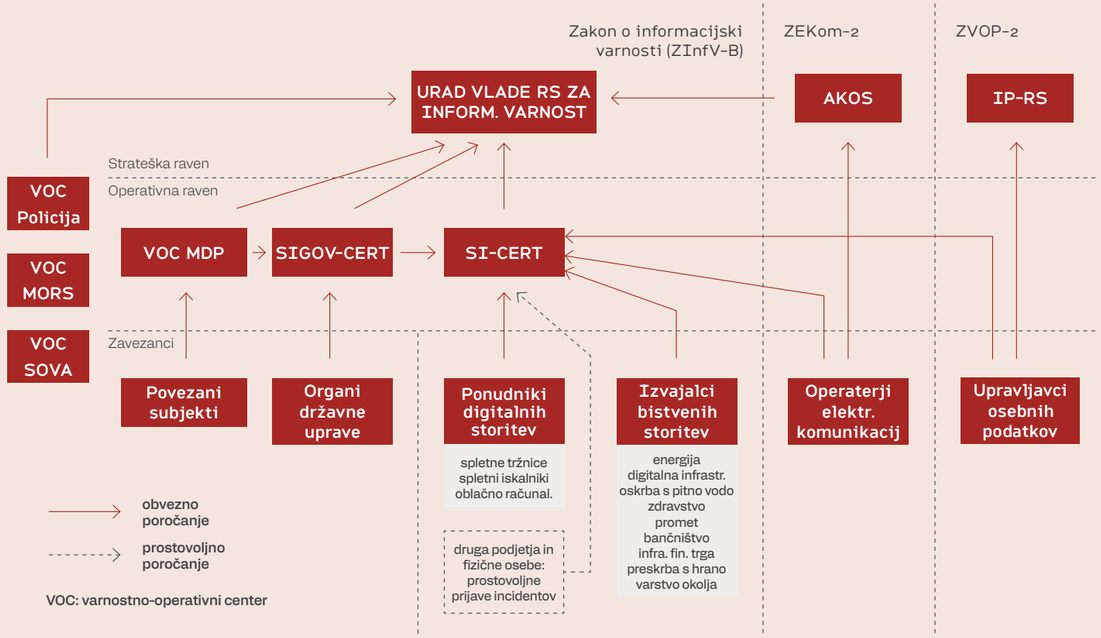
1 Zavezanci po Zakonu o informacijski varnosti so tako izvajalci bistvenih storitev kot ponudniki digitalnih storitev, ki morajo nacionalnemu CSIRT brez nepotrebnega odlašanja priglasiti incidente s pomembnim negativnim vplivom na delovanje bistvenih storitev, ki jih zagotavljajo. Pri določitvi, ali 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 (ZVOP-2), 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.

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.

NACIONALNI OKVIR KIBERNETSKE VARNOSTI



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 podatke 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.

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 bil septembra 2023 povabljen k sodelovanju 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 ter orodij in merljivo zmanjšanje kibernetskih 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 kibernetske varnosti partnerji pridobijo tudi dostop do globalne mreže sodelovanja in izmenjave informacij. Sodelovanje v GCA partnerjem omogoča, da aktivno prispevajo k oblikovanju kibernetske politike in strategij ter se učinkovito odzovejo na nove kibernetske grožnje.

SODELOVANJE PRI EVROPSKIH PROJEKTIH

Strokovni sodelavci SI-CERT smo poleg rednega dela aktivni tudi na posebnih raziskovalno-inovacijskih projektih, kjer z deljenjem znanja in sodelovanjem z deležniki iz drugih sektorjev, kot je na primer energetika, spoznavamo specifike sektorskih subjektov. Trenutno smo tako del evropskega konzorcija 26 partnerjev iz osmih evropskih držav, kjer pod mehanizmom Obzorje 2020 poteka projekt, imenovan CyberSEAS. Projekt se je začel oktobra 2021 in bo trajal do konca septembra 2024.

Projekt, ki ga sofinancira Evropska komisija, naslavlja izzive kibernetske varnosti v evropskih energetskih sistemih, kako izboljšati splošno odpornost energetskih dobavnih verig, jih zaščititi pred motnjami, ki izkoriščajo izboljšane interakcije, modele razširjene vključenosti deležnikov (prosumer) in potrošnikov (consumer) kot kanale za kompleksne kibernetske napade, prisotnost podedovanih sistemov in vse večjo povezljivost energetskih infrastruktur, shramb podatkov in trgovcev na drobno s storitvami.

Pri projektu sodelujemo tako partnerji iz zasebnega, javnega in energetskega sektorja kot univerze. Slovenskih partnerjev je pet, poleg SI-CERT-a še Petrol, d. d., Informatika, d. d., Operato in Inštitut za korporativne varnostne študije ICS. SI-CERT sodeluje pri razvoju in izboljšanju procesov prijave in zaznave potencialnih incidentov ter pri iskanju rešitve, kako optimizirati izmenjavo občutljivih podatkov in informacij med prijavitelji in SI-CERT-om.

Ključni rezultat projekta CyberSEAS bo 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.

Udeležba SI-CERT pri projektu prinaša prednosti na področju umeščanja rešitev na področje zakonodajne skladnosti in splošno ustaljenih procesov v skupnosti CSIRT. V pilotnem delu SI-CERT sodeluje s platformo MISP, ki omogoča izmenjavo podatkov o kibernetskih grožnjah in prispeva k širši uporabnosti končnih rešitev. Scenarije pilotov in programske rešitve smo tako uskladili na združljivost s platformo MISP, ki je široko razširjena v CSIRT in kibernetski varnostni skupnosti.

IZMENJAVA INFORMACIJ O KIBERNETSKIH GROŽNJAH

MISP (Malware Information Sharing Platform) je odprtokodna platforma za izmenjavo informacij o kibernetskih grožnjah. Prek platforme MISP partnerji izmenjujemo informacije o kazalnikih zlorab (IoC), pridobljenih z analizo škodljive kode ali zajemom in analizo sumljive omrežne dejavnosti. Tako pridobljeni indikatorji so ključnega pomena pri pravočasnem odkrivanju in proaktivni zajezitvi omrežnih zlorab ter tudi za povezovanje posameznih, z analizo pridobljenih indikatorjev z že znanimi omrežnimi zlorabami in okužbami.

Na SI-CERT upravljamo centralno vozlišče MISP v državi in smo dobro povezani v mednarodno skupnost. S priklopom na platformo MISP organizacije pridobijo brezplačen dostop do širokega nabora indikatorjev zlorab, ki jih lahko uporabijo za iskanje korelacij znotraj sistema SIEM ali pa zgolj kot dodatna pravila na požarni pregradi ali obogatitev filtrov poštnega strežnika.

SI-CERT se je globalni skupnosti MISP aktivno pridružil pred skoraj desetimi leti. V preteklih desetih letih smo skrbeli za vpeljavo platforme MISP v lokalni skupnosti in pri širitvi platforme MISP v druge države bližnje regije, kjer predstavljamo stičišče za izmenjavo s skupinami CSIRT na območju Zahodnega Balkana.

K uporabi platforme MISP želimo spodbuditi čim več **zavezancev po Zakonu o informacijski varnosti, podatke izmenjave lahko namreč povežejo v svoje sisteme SIEM in sporočene indikatorje upoštevajo pri zaščiti svojega omrežja.**

KLJUČNE ŠTEVILKE V LETU 2023

20 — povezanih subjektov v Sloveniji

na platformo dodanih več kot — **35.000** — novih dogodkov

SI-CERT delil — **86** — dogodkov

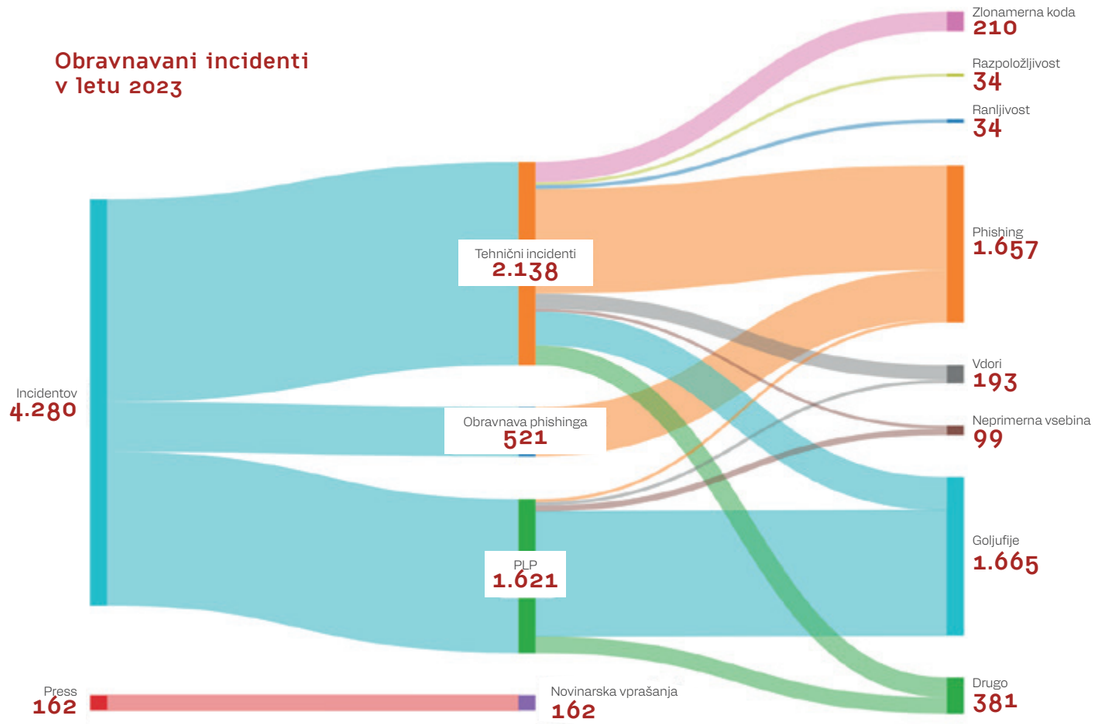
VRSTE, ŠTEVILO INCIDENTOV IN KLJUČNI KAZALCI

TRI LINIJE OBRAVNAVE

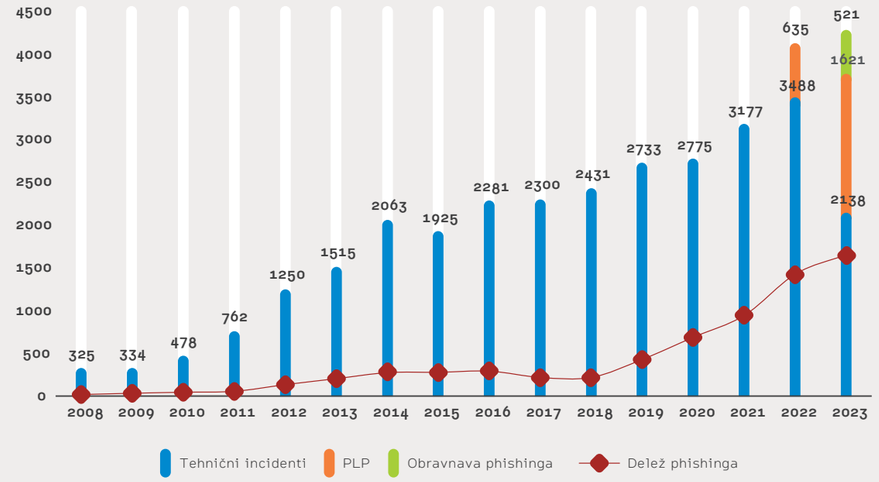
Leta 2022 smo na SI-CERT uvedli prvolinijsko podporo (PLP) za obravnavo tehnično manj zahtevnih incidentov. Porast phishing napadov v zadnjih nekaj letih pa nas je spodbudil, da smo začeli z zasnovo, preizkušanjem in nato konec avgusta 2023 tudi vpeljavo posebne linije za ločeno obravnavo tudi teh. Namen te je optimizacija postopkov, ki bodo skrajšali čas obdelave podatkov in izvedbe potrebnih ukrepov. Projekt bo predvidoma končan leta 2024.

V letu 2023 smo tako obravnavali 4.280 incidentov, ki jih peljemo skozi tri različne postopke:

- tehnično zahtevnejši incidenti,
- obravnava phishing napadov,
- prvolinijska podpora (tehnično manj zahtevni incidenti). (PLP)



INCIDENTI SKOZI LETA



PRIJAVITELJI PO SEKTORJIH

924 (12%)
fizična oseba

606 (12%)
druge pravne osebe

269 (12%)
bančništvo

116 (5%)
raziskovanje in izobraževanje

60 (3%)
državni organi

40 (2%)
operater elektronskih komunikacij

22 (1%)
zdravstvo

20 (1%)
energija

20 (1%)
promet

6 (0%)
digitalni trg

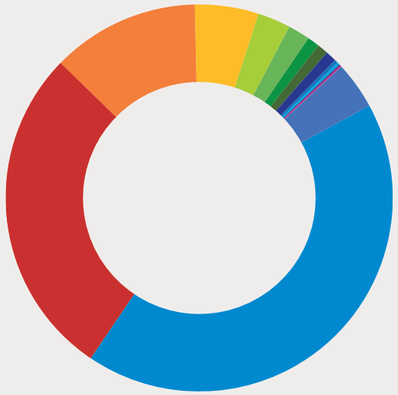
5 (0%)
digitalna infrastruktura

2 (0%)
pitna voda

2 (0%)
oblačno računalništvo

1 (0%)
finančni trgi

86 (4%)
drugo



KLJUČNE BESEDE V OBRAVNAVANIH INCIDENTIH

VRSTE INCIDENTOV

Skupina	Vrsta incidenta	2020	2021	2022	2023
Neprimerna vsebina	Neželena sporočila	72	120	97	92
	Žaljiva vsebina	22	13	9	7
	Nasilna vsebina	3	0	1	0
Zlonamerna koda	Virus	46	29	8	9
	Črv	0	2	0	2
	Trojanski konj	141	171	278	140
	Vohunska programska oprema	1	2	2	1
	Samodejni izbirnik (ang. dialler)	0	0	0	1
	Korenski komplet (ang. rootkit)	1	0	0	1
	Boti in botneti	16	9	8	4
	Nadzorni strežnik	7	0	1	0
	Izsiljevalski virus	69	64	45	32
	Orodje za oddaljen nadzor (RAT)	14	29	33	22
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	28	41	42	22
	Prestrezanje komunikacije	1	1	0	1
	Socialni inženiring	2	0	3	0
Poskusi vdora	Izkoriščanje znane ranljivosti	4	1	3	5
	Poskusi prijav, napad z grobo silo (ang. brute force attack) in napadi s slovarjem	16	32	18	24
	Nova vrsta napada	0	0	0	0
Vdori	Zloraba privilegiranega uporabniškega računa	7	6	0	3
	Zloraba neprivilegiranega uporabniškega računa	82	105	112	150
	Napad na aplikacijo	4	5	6	11
Razpoložljivost	Napad onemogočanja	7	6	5	5
	Porazdeljen napad onemogočanja	31	27	17	21
	Sabotaža	0	0	0	1
	Izpad delovanja naprav ali omrežja	2	4	1	7
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	13	12	8	4
	Nepooblaščeno spreminjanje podatkov	8	22	15	18
	Odtekanje informacij	5	6	5	5
Goljufije	Nepooblaščeno izkoriščanje virov	4	5	6	13
	Intelektualna lastnina in avtorske pravice	10	10	12	2
	Kraja identitete	67	68	48	65
	Phishing sporočilo	488	765	1221	1610
	Phishing spletno mesto	202	185	211	47
	Spletno nakupovanje	97	86	113	286
	Goljufija z vnaprejšnjim plačilom	168	182	181	177
	Izsiljevanje	144	138	346	329
	Druge goljufije	668	655	762	760
Ranljivosti	Odgovorno razkrivanje	14	12	4	9
	Razkritje ranljivosti	2	12	53	20
	Ranljivi sistemi in naprave	20	33	15	13
Drugo	Drugo	226	301	320	347
	Novinarsko vprašanje	53	9	1	0
Test	Namenjeno preizkusom	1	1	1	2
Skupaj		2766	3169	4011	4268
Nerazvrščenih		9	8	112	12
Vseh incidentov		2775	3177	4123	4280

V tabeli Razvrstitev incidentov je razviden upad novinarskih vprašanj, ki pa je samo navidezen in je posledica tega, da smo v začetku leta 2021 spremenili njihovo obravnavo: uvedli smo naslov press@cert.si in ločeno linijo za odgovore. Skupaj smo (vključno z zgoraj navedenim) v letu 2023 prejeli 162 novinarskih vprašanj

VIŠINA OŠKODOVANJ

140.000€
najvišje oškodovanje
pri investicijski prevari
s kriptovalutami

42.000€
povprečno oškodovanje
v direktorski prevari
(CEO Fraud)

40.000€
povprečno oškodovanje
pri investicijski prevari

30.000€
povprečno oškodovanje
pri vrivanju v poslovno
komunikacijo (BEC)

20.000€
najvišje oškodovanje
v ljubezenski prevari

5.000€
povprečno oškodovanje v prevari
z vnaprejšnjim plačilom (znani
tudi kot nigerijska prevara)

1.030€
povprečno oškodovanje pri
spletnem nakupovanju

ODZIVNI ČAS SI-CERT V LETU 2023

Morda lahko že sklepamo, da sta uvedbi specializiranih linij za obravnavo prvolinijskih prijav in phishinga prinesli prve rezultate. Odzivni čas SI-CERT-a se je namreč v primerjavi z letom 2022 izboljšal in večji delež odgovorov pošljemo v prvi in drugi uri od prijave. V izračunu seveda niso upoštevani samodejni odgovori, ampak samo dejanski odgovori zaposlenih na SI-CERT ob prijavi incidenta.

odgovor poslan v
eni uri
27%

odgovor poslan v
dveh urah
41%

odgovor poslan v
12 urah
66%

odgovor poslan v
24 urah
87%

POMEMBNEJŠE DEJAVNOSTI IN OPAŽANJA

OBRAVNAVA RANLJIVOSTI

Ranljivost je niz različnih pogojev, ki omogočajo kršitev varnostne politike. Gre za pomanjkljivosti v informacijskem sistemu, aplikacijah, omrežnih napravah, varnostnih postopkih sistema, notranjem nadzoru ali izvajanju postopkov, ki so lahko predmet izkoriščanja ali zlorabe. Ranljivost lahko povzročijo napake v programski opremi, napačna konfiguracija ali nepričakovane interakcije med različnimi sistemi. Uspešno izkoriščanje ranljivosti ima lahko za posledico tehnična tveganja in tudi tveganja, ki lahko ogrozijo celoten sistem.

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 na elektronski novičnik Odziv.

OBJAVLJENA VARNOSTNA OBVESTILA V LETU 2023

Oznaka	Opis	CVSS
SI-CERT 2023-01	Uhajanje NTLM poverilnic prek Outlook ranljivosti	9,8
SI-CERT 2023-02	Zloraba dobavne verige: 3CX Electron DesktopApp	-
SI-CERT 2023-03	Ranljivost FortiOS in FortiProxy / CVE-2023-27997	9,8
SI-CERT 2023-04	Ranljivosti Citrix/NetScaler ADC in Gateway	9,8
SI-CERT 2023-05	Ranljivost Ivanti Endpoint Manager Mobile (MobileIron)	10,0
SI-CERT 2023-06	Zlorabe Cisco IOS XE naprav	10,0

Objavljena opozorila se običajno nanašajo zgolj na zelo resne ranljivosti, ki bi lahko povzročile veliko škodo in ki se ponavadi že izrabljajo v napadih. Take ranljivosti zahtevajo zelo hitro ukrepanje upravljavcev sistemov, popravki zanje pa so izdani mimo rednih ciklov izdajanja popravkov. Zato o njih pogosto obveščamo tudi neposredno skrbnike sistemov oziroma uporabnike, za katere pridobimo informacijo, da so njihovi sistemi ranljivi.

Kam pošljemo obvestilo, je odvisno od vrste podatkov. Če je identifikator ranljivega sistema domena, lahko obvestimo tehnični kontakt nosilca domene, v primeru naslova IP pa tehnični ali »abuse« kontakt, ki je naveden v RIPE Whois bazi za naslovni prostor, ki mu pripada naslov IP. Običajno gre za množično obveščanje, pri pošiljanju pa si pomagamo s skriptami. Žal kontaktni podatki niso vedno posodobljeni in aktualni, zato se del poslanih obvestil vrne v obliki obvestila o nedostavljenem sporočilu. Vse take primere moramo dodatno ročno preveriti in poiskati drug ustrezen kontakt.

Kaj je CVE?

CVE (Common Vulnerabilities and Exposures) je javno dostopen seznam ranljivosti programske opreme. Vsaki ranljivosti v seznamu CVE je dodeljen edinstven identifikator, imenovan CVE ID, ki je sestavljen iz leta in številke (npr. CVE-2023-20198).

Kaj je CVSS?

CVSS (Common Vulnerability Scoring System) je standard za ocenjevanje resnosti ranljivosti programske opreme. CVSS ocena je določena na podlagi več dejavnikov, na primer načina in kompleksnosti izrabe, vpliva na zaupnost, integriteto in razpoložljivost podatkov ipd. Sega od 0 do 10, pri čemer ocena 10 pomeni največjo možno resnost.

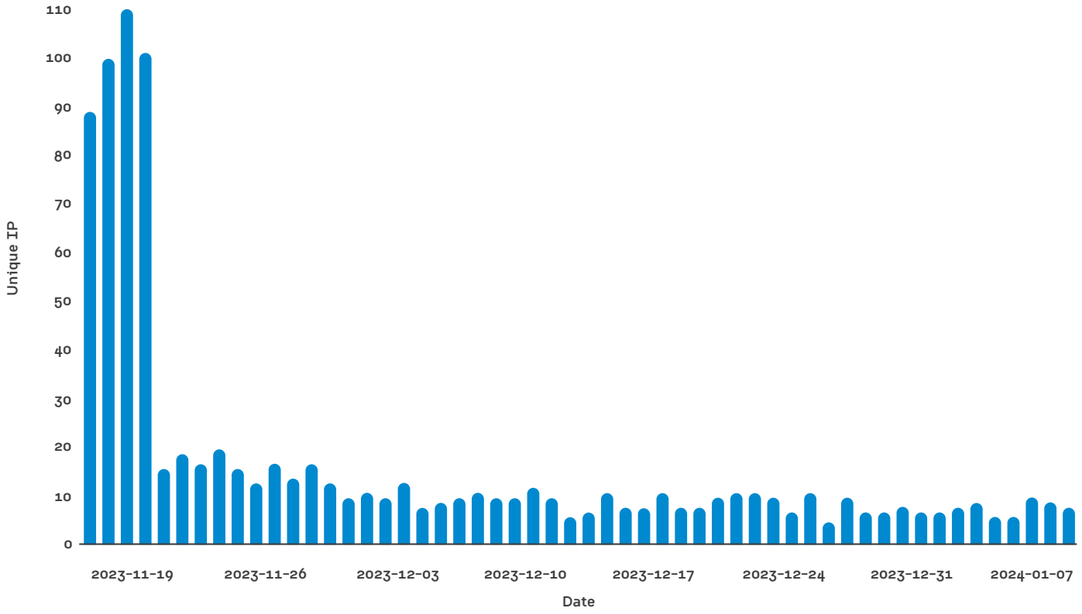
Skrbniki sistemov bi morali poskrbeti, da so kontaktni naslovi vedno aktualni.

Aktualne kontaktne podatke o omrežjih lahko preverite na spletni strani RIPE Database https://apps.db.ripe.net/db-web-ui/query ali s pomočjo ukaza »whois«.

Primer iskanja kontaktnega naslova za prijavo zlorab za IP naslov 193.2.1.34:

```
$ whois -b -h whois.ripe.net 193.2.1.34
inetnum: 193.2.1.0 - 193.2.1.255
abuse-mailbox: abuse@arnes.si
```

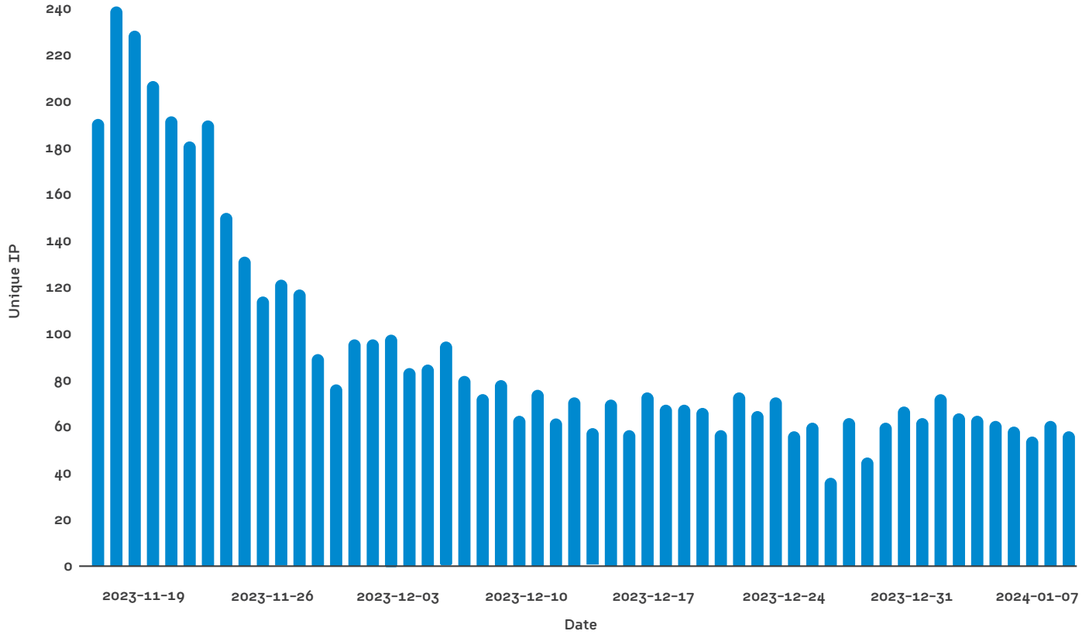
Pri obravnavi in obveščanju o ranljivostih lahko včasih spremljamo tudi časovni potek odpravljanja ranljivosti. Pri tem vedno naletimo na pojav t. i. dolgega repa, saj kljub različnim vrstam obveščanja število ranljivih sistemov nikoli ne pade na 0. Želimo si, da bi število ranljivih sistemov hitro padalo, kot na primer pri obveščanju o nepodprtih Exchange strežnikih.



Graf prikazuje število nepodprtih strežnikov Exchange v Sloveniji

Včasih pa je hitrost padanja precej majhna, kar ni zaželeno, kot na primer pri obveščanju o Exchange ranljivosti CVE-2023-36439.

SI-CERT novice in obvestila o pomembnih ranljivostih lahko spremljate tudi prek RSS kanala (https://cert.si/rss) ali prek SI-CERT novičnika ODZIV, na katerega se lahko naročite na spletni strani https://cert.si. Širši javnosti je namenjen novičnik Varne novice, na katerega se naročite na https://varninainternetu.si. Prek njega pošiljamo obvestila o aktualnih spletnih goljufijah in nasvetih za večjo varnost na spletu.



Graf prikazuje število Exchange strežnikov v Sloveniji, ranljivih na CVE-2023-36439

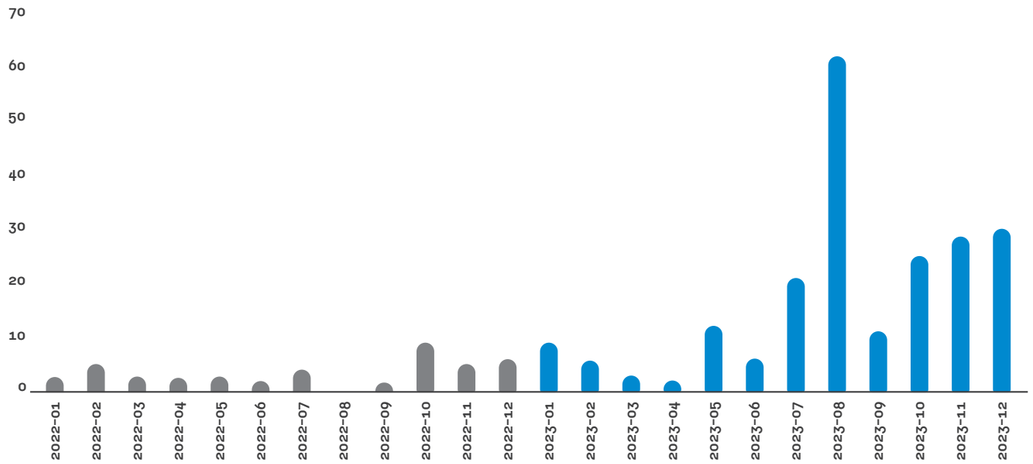
OBVEŠČANJE OPERATERJEV O OKUŽENIH SISTEMIH NJIHOVIH UPORABNIKOV

Na SI-CERT smo v letu 2023 začeli obveščati operaterje elektronskih komunikacij o okuženih napravah naročnikov njihovih storitev. V največ primerih gre za sisteme domačih uporabnikov. Podatke nam pošljejo partnerske organizacije, ki z različnimi metodami pridobijo podatke o okuženih sistemih in jih posredujejo nacionalnim odzivnim centrom po različnih državah. Podatke pošiljamo operaterjem enkrat tedensko, operaterje pa prosimo, da na podlagi prejetih podatkov identificirajo uporabnike okuženih sistemov in jih obvestijo o zlorabi. Informacije se nanašajo na različne vrste okužb, od najnovejših pa do starejših, ki lahko tudi ne predstavljajo več resne grožnje.

Računalniški črv Conficker se je prvič pojavil leta 2008 in bil zelo aktiven leta 2009. Čeprav je od pojava virusa minilo že več kot 15 let in ga vsi antivirusni programi prepoznajo in odstranijo, je še vedno prisoten, predvsem v zelo starih sistemih, ki morajo iz določenih razlogov še vedno delovati, vendar pa jih ni več mogoče posodabljati. Konec leta 2023 smo tako imeli v Sloveniji še vedno 39 okuženih sistemov z virusom Conficker.

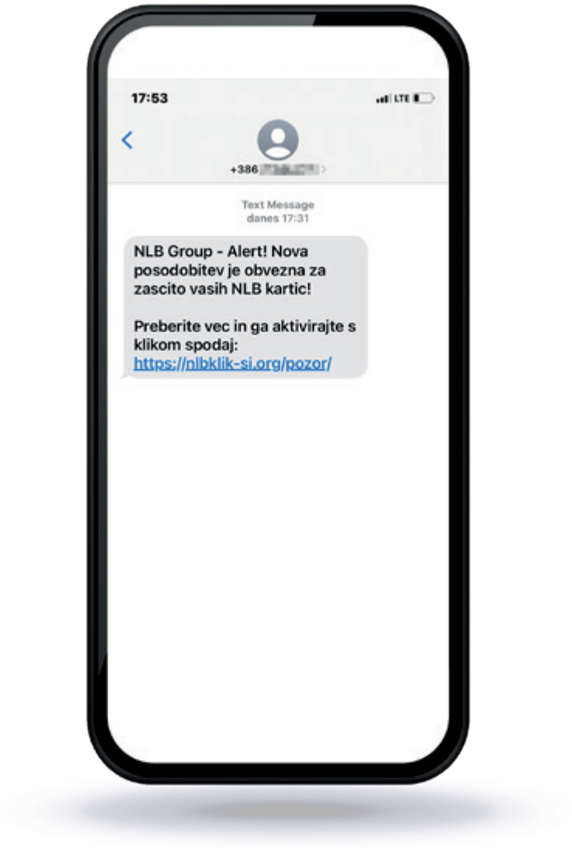
VZPON SMISHINGA

Smishing napade na SI-CERT-u obravnavamo redno. Jeseni 2022 in v začetku leta 2023 smo opazili manjše povečanje prijav, veliko prijav pa je prišlo konec julija 2023 in se nadaljevalo v avgust. In kaj pravzaprav je smishing? Ribarjenje ali phishing je dokaj preprosta goljufija, kjer vas storilci želijo zavesti v obisk lažnega spletnega mesta banke, pošte, spletne prodajalne ali spletne pošte, kjer boste vpisali uporabniško ime in geslo, misleč, da morate »posodobiti podatke« za storitev, v resnici pa tako svoje geslo pošljete goljufom. Ti sporočila pošiljajo najpogosteje po elektronski pošti, lahko pa tudi v SMS-sporočilih. Takrat to imenujemo smishing. Omenjeni porast prijav je dobro viden na grafu mesečno obravnavanih smishing incidentov na SI-CERT.



Mesečno število lažnih SMS-sporočil (smishing) na SI-CERT (do 15. avgusta 2023)

Navadno so SMS-sporočila poslana s potvorjeno izvorno številko (proti temu se mobilni operaterji sproti prilagajajo z ustreznimi ukrepi preprečevanja, zato so ti primeri vedno redkejši) ali pa iz tuje številke. Konec julija 2023 pa smo na SI-CERT začeli prejemati val prijav SMS-sporočil, ki so bila poslana iz slovenskih številk.



Primer smishing sporočila iz 29. julija 2023

Ob vsaki prijavi phishing napada na SI-CERT sprožimo postopke za odstranitev lažnega spletnega mesta in hkrati za njegovo uvrstitev na zadrževalne sezname (Googlov Safe Browsing List in Microsoftov Smart Screen). V tem primeru smo takoj stopili tudi v stik z operaterji mobilne telefonije v Sloveniji, jih opozorili na običajne poteke napadov in jim ažurno posredovali številke, ki so bile uporabljene za razpošiljanje zlonamernih sporočil. Ko smo od operaterjev dobili tudi potrditev, da gre dejansko za razpošiljanje z naprav s SIM-karticami, kupljenimi v Sloveniji, smo naše ugotovitve in seznam uporabljenih številk poslali slovenski policiji. Ta je na podlagi predhodnih prijav s strani bank in drugih pridobljenih ugotovitev 10. avgusta v Mariboru aretirala štiri romunske državljane.

Po tem avgustovskem incidentu se število zaznanih smishing napadov ni vrnilo na prejšnjo raven, kar pripisujemo vedno širši uporabi mobilnih denarnic v Sloveniji.

Za aktivacijo mobilne denarnice so namreč dostikrat potrebni zgolj štirje podatki, ki jih napadalci pridobijo med različnimi phishing in drugimi napadi: telefonska številka, davčna številka, enkratna koda iz prejetega SMS-sporočila in PIN-koda bančne kartice. S temi podatki lahko napadalci na svoji mobilni napravi namestijo in aktivirajo mobilno denarnico v imenu žrtve ter prek nje opravljajo in potrjujejo različne spletne nakupe.

ŠKODLJIVA KODA

Na področju zlonamerne kode leto 2023 ni prineslo izstopajočih sprememb. Še vedno smo se najpogosteje ukvarjali z različnimi trojanskimi konji, izsiljevalskimi kriptovirusi in orodji za oddaljen dostop. Pri trojanskih konjih prednjači AgentTesla, sledi mu FormBook oziroma xLoader, med orodji za oddaljen dostop pa močno prevladuje Remcos. Druge vrste obravnavanih virusov so v manjšini.

Vrste škodljive kode – pregled 2023

Vrsta škodljive kode	Št. obravnavanih primerov
Trojanski konj	140
Ransomware	32
Orodje za oddaljen nadzor	22
Drugo	18

Najpogostejši trojanski konji skozi leta

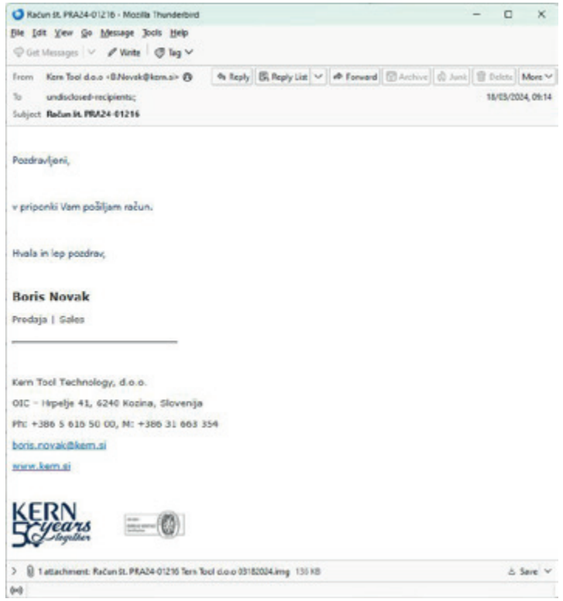
Leto	AgentTesla	FormBook
2020	4	4
2021	33	39
2022	67	90
2023	63	44

Računalniški virusi se še vedno najpogosteje širijo v obliki priponk elektronske pošte s sporočili, ki želijo naslovnika prepričati, da nanjo klikne in s tem namesti zlonamerno kodo. Lažna sporočila postajajo čedalje prepričljivejša in jih je včasih že zelo težko prepoznati. Lahko vsebujejo elemente pretekle korespondence, z različnimi tehnikami pa tudi preslepijo filtre poštnih strežnikov. Taka lažna sporočila običajno predstavljajo prvi korak pri nepooblaščenem dostopu do omrežja podjetja skozi okužbo računalnika enega od zaposlenih. Proces okužbe praviloma vsebuje več stopenj, od prenosa dodatne kode iz oddaljenega strežnika do izvedbe različnih vmesnih skript.

Vektor zlorabe okužbe je lahko tudi slabo zaščiten sistem za oddaljen dostop (na primer zaščita zgolj z geslom brez 2FA) ali pa ranljivost javno dostopnega strežnika v primeru neustrezne politike posodabljanja sistemov.

ŠIRJENJE LAŽNIH SPOROČIL V IMENU SLOVENSKIH ORGANIZACIJ

V letu 2023 smo obravnavali več napadov z lažnimi elektronskimi sporočili, ki so na prvi pogled izgledala kot legitimna sporočila različnih slovenskih organizacij, največkrat podjetij, bank in izobraževalnih ustanov. Napadalci najverjetneje v nekem zlorabljenem poštnem predalu ukradejo eno izmed poslanih ali prejetih sporočil, ki ga modificirajo na tak način, da priložijo škodljivo priponko, večine drugih elementov pa ne spremenijo. Pri pošiljanju lahko tudi ponaredijo elektronski naslov pošiljatelja, tako da na prvi pogled lahko izgleda, da ga je poslala neka organizacija.



Postranska žrtev takega napada je tudi organizacija, v imenu katere napadalci pošiljajo lažna sporočila. Ta se mora običajno spopasti s povratnimi sporočili in telefonskimi klici jeznih prejemnikov, ki ne razumejo, da lažnega sporočila ni poslala organizacija.

Organizacije se lahko pred ponarejanjem elektronskih sporočil iz njihove domene zavarujejo z nastavitvijo naslednjih varnostnih protokolov za preverjanje pristnosti e-pošte:

- SPF (Sender Policy Framework) omogoča določitev poštnih strežnikov, ki se lahko uporabljajo za pošiljanje pošte iz domene;
- DKIM (Domainkeys Identified Mail) omogoča preverjanje pristnosti sporočila z uporabo kriptografske avtentikacije;
- DMARC (Domain-based Message Authentication, Reporting & Conformance) omogoča nastavitev pravil za obravnavo sporočil, ki ne prestanejo SPF in DKIM preverjanja.

NAPADI NA PODJETJA

Pogosta tarča kibernetskih napadalcev so majhna in srednja podjetja, saj velikokrat nimajo možnosti zagotavljanja zadostnih virov za zagotavljanje odpornosti na kibernetska tveganja. Po drugi stani pa je njihovo poslovanje zelo odvisno od razpoložljivosti podatkov in nemotenega delovanja informacijskega sistema. Uspešen kibernetski napad lahko za daljše časovno obdobje ustavi poslovanje podjetja, kar lahko pomeni velike izgube, ki jih podjetje težko nadomesti. Podjetja so zelo izpostavljena napadom z izsiljevalskimi virusi, ki po vdoru v informacijski sistem zašifrirajo vse dosegljive datoteke. Napadalci žrtvam ponudijo možnost odkupa šifrirnega ključa, pri čemer znesek odkupnine prilagodijo velikosti podjetja. Običajni zneski odkupnine so od nekaj 10.000 do več milijonov evrov.

NOV SCENARIJ DIREKTORSKE PREVARE

Direktorska prevara (ang. CEO fraud) je preprosta oblika napada, pri kateri napadalci na različne načine prevzamejo identiteto člana vodstvenega kadra (običajno direktorja) ter v njegovem imenu od drugih zaposlenih zahtevajo izvedbo določenih nalog, ki pa so v škodo podjetja. Značilen primer direktorske prevare je pošiljanje elektronskega sporočila na naslov računovodstva z zahtevo po nujnem plačilu izmišljene fakture na nek tuj bančni račun, pri čemer gre za zneske v višini nekaj 10.000 evrov. Napadalci lahko registrirajo tudi elektronski naslov, ki vsebuje ime in priimek direktorja, ali pa pri pošiljanju sporočila ponaredijo pošiljatelja (t. i. email spoofing). Naprednejši napadi te vrste lahko vsebujejo tudi avdio- in videoposnetke, ustvarjene z orodji umetne inteligence, vendar pa so na srečo taki napadi v Sloveniji (še) izredno redki.

V letu 2023 so napadalci v direktorski prevari začeli uporabljati nov scenarij. Na naslov računovodstva pošljejo lažno sporočilo enega od zaposlenih, da želi nakazilo plače na drug bančni račun. Zneski oškodovanja so v tem primeru manjši, po nakazilu plače na drug bančni račun pa je možnost povrnitve ukradenega denarja zelo majhna.

Vrivanje v poslovno komunikacijo (ang. BEC, business email compromise) je naprednejša oblika kibernetskega napada, ki zahteva predhodni vdor v poštni sistem podjetja. Ta je običajno posledica uspešnega phishing napada na zaposlene. Z vdorom v poštni predal napadalci spremljajo komunikacijo v podjetju in ob pošiljanju fakture v njej zamenjajo podatek o bančnem računu in tako preusmerijo nakazilo denarja. Zneski oškodovanja so praviloma zelo visoki.

Kakršnokoli spremembo v načinu izplačevanja vedno preverite po neodvisnem kanalu (osebno, po telefonu ipd.). Zaposleni se lahko o direktorski prevari in vdoru v poslovno komunikacijo seznanijo na brezplačnem spletnem tečaju o informacijski varnosti Varni v pisarni, ki smo ga pripravili na SI-CERT.

Leto	BEC	CEO fraud
2019	35	128
2020	40	32
2021	52	25
2022	41	36
2023	37	73

IZSILJEVALSKI VIRUSI

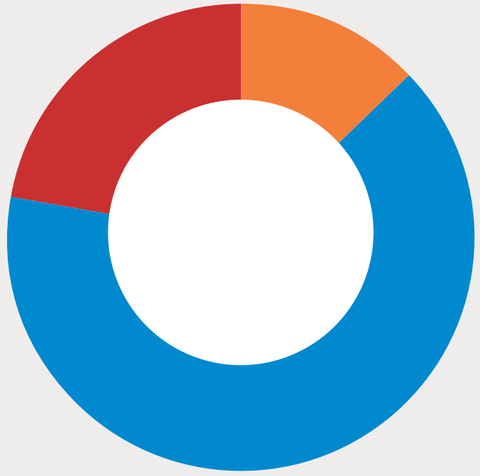
Ransomware ali izsiljevalski virusi so ena izmed največjih kibernetskih groženj. Po zlorabi sistema zašifrirajo vse dokumente, do katerih imajo dostop, tudi na omrežnih in priključenih pogonih, za šifrirni ključ pa zahtevajo odkupnino, ki je velikokrat odvisna od velikosti podjetja, običajno pa znaša od nekaj 10.000 do več milijonov evrov. Po obdobju napadov na fizične osebe v letih 2016 do 2019 se je glavnina napadalcev usmerila na podjetja, saj lahko tam napadalci računajo na večje zneske odkupnine. Izsiljevanje velikokrat vsebuje tudi grožnjo z javno objavo ukradenih podatkov ali pa celo izsiljevanje poslovnih partnerjev podjetja. Glavni vstopni vektor je slaba oziroma neustrezna zaščita sistema za oddaljen dostop ali pa kraja avtentikacijskih podatkov za oddaljen dostop, vključno z VPN-poverilnicami.

Število obravnavanih napadov z izsiljevalskimi virusi v zadnjih letih postopoma upada. V 32 obravnavanih primerih v letu 2023 smo identificirali 18 različnih vrst virusov, pri čemer sta bila v tretjini vseh primerov uporabljena Phobos in Akira.

Leto	Št. primerov okužbe z izsiljevalskim virusom
2016	212
2017	171
2018	64
2019	53
2020	69
2021	64
2022	45
2023	32

Pri identifikaciji vrste izsiljevalskega virusa in možnosti restavriranja datotek brez plačila odkupnine sta žrtvam v pomoč iskalnika na https://www.nomoreransom.org/ in https://id-ransomware.malwarehunterteam.com/. Priporočila SI-CERT so na voljo v tehničnem zapisu 11: https://cert.si/tz011.

PRIJAVITELJI



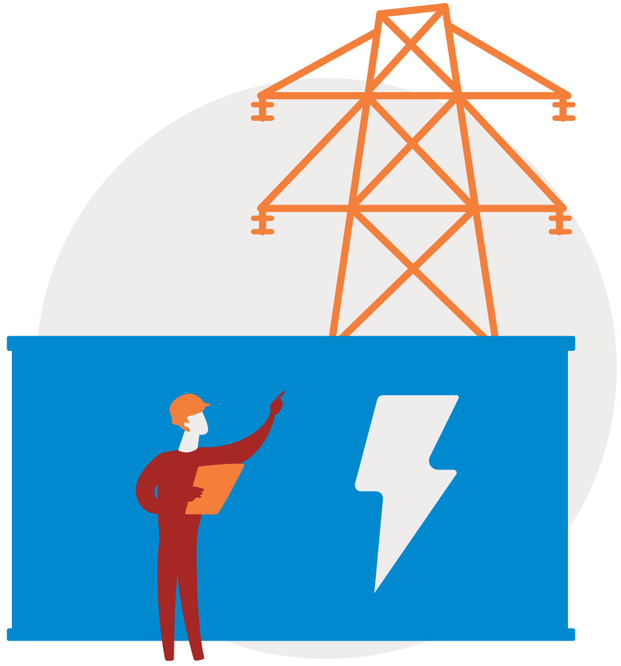
13%
4
Zasebni uporabniki

65%
21
Podjetja

22%
7
Izobraževalne ustanove

NAPAD NA HOLDING SLOVENSKIH ELEKTRARN

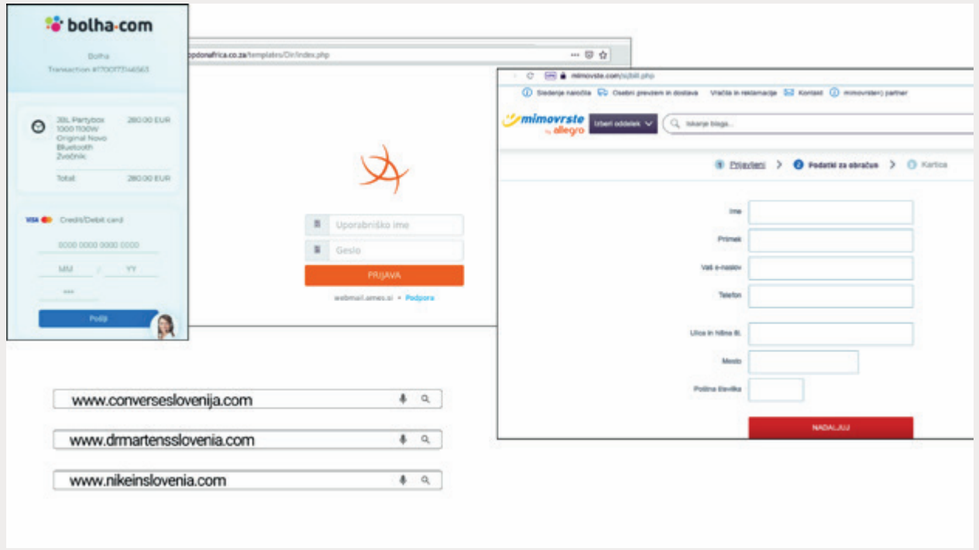
Konec novembra 2023 je HSE, Holding Slovenskih elektrarn prizadel izsiljevalski virus Ryshida. Napadalci so izkoristili oddaljen dostop, namenjen zunanjemu izvajalcu. Kadar pride do okužbe sistema in kraje poverilnic, je to ena od možnih poti v sistem. Ob hitrem ukrepanju strokovnih služb HSE je storilcem uspelo zašifrirati le manjši del sistemov in pridobiti dostop do podatkov, ki niso imeli posebne vrednosti. Vse sisteme so ponovno postavili iz varnostnih kopij in ob dodatnih varnostnih ukrepih. Oskrba z električno energijo v nobenem trenutku zaradi napada ni bila motena.



NOVI PRISTOPI SPLETNIH GOLJUFOV

V letu 2023 smo spet zaznali rast števila incidentov, pri čemer ostaja že nekaj let precej stabilno razmerje, da spletne prevare predstavljajo tretjino vseh obravnavanih primerov. V skoraj 30 letih delovanja SI-CERT imamo že toliko vpogleda v problematiko, da lahko izpostavimo nove pristope spletnih napadalcev, ki smo jih zaznali.

Gotovo vidimo **trend lokalizacije**, saj napadalci vedno pogosteje za svoje krinke izrabljajo slovenske storitve in podjetja, ki so slovenskim uporabnikom blizu in tudi vzbujajo več zaupanja. Tako smo zaznali več phishing napadov, kjer so zlorabili podjetja Mimovrste, Bolha.com, Pošta Slovenije, Arnes elektronsko pošto ipd. Slovenščina v napadih je vedno boljša in prepričljivejša, kar je posledica zmogljivih prevajalskih programov. Podoben trend je tudi pri lažnih spletnih trgovinah, ki zavajajo, da gre za slovenske trgovce oziroma slovenske distributerje, na način, da v imenu spletne trgovine uporabljajo ime Slovenija ali Ljubljana. Celo na družbenih omrežjih za vabe v prevaro s skrito naročnino pogosto izrabijo znane slovenske vplivneže in zvezdnike.



Prav tako vidimo, da napadalci žrtvam posvetijo vedno več časa. **Napadi so vse bolj personalizirani in prilagojeni posamezni žrtvi.** Vse več je napadov z neposrednim stikom, torej napadalci žrtev pokličejo po telefonu ali kontaktirajo prek zasebnega sporočila (Viber, Telegram). Vzamejo si veliko časa za prepričevanja in pojasnila. Izstopajo predvsem kripto investicijske prevare, kjer napadalci za prepričljivejšo krinko organizirajo spletne seminarje, snemajo videonavodila, upravljajo zaprte podporne skupine, ki zahtevajo veliko vloženega napora.

Napadi postajajo vse bolj **prilagojeni telefonom in našim uporabniškim navadam (*t. i. mobile first*)**. Opazili smo velik skok v številu napadov prek SMS-sporočil in aplikacij za hipno sporočanje (na primer Viber, WhatsApp). Nevarnosti se selijo na pametne telefone v obliki zasebnih sporočil, ki pod pretvezo »preverjanja podatkov«, »potrjevanja transakcij« ipd. želijo izvabiti podatke za dostop do elektronske banke in podatke kreditne kartice (t. i. smishing). Ti napadi prek SMS-sporočil so za uporabnike lahko nevarnejši od napadov prek elektronske pošte, saj pred slednjimi lahko ščitijo filtri na poštnih strežnikih, ki blokirajo del zlonamernih sporočil. Praktično nemogoče je preveriti pošiljatelja SMS-sporočila, možno pa je tudi potvoriti telefonske številke, da izgledajo, kot da so slovenske. V SMS-sporočilu je tudi težje preveriti, kam pelje povezava, kot to lahko storimo na računalniku. Hkrati pa je celotno besedilo manjše in težje berljivo kot na računalniškem zaslonu, kar je še dodatna ovira za starejše uporabnike. Ne nazadnje je tudi način uporabe telefona veliko bolj oseben, pogosto ga uporabljamo v okolju, kjer si težje vzamemo trenutek miru, da natančno preverimo stran, kamor vnašamo podatke.

Izpostavljamo tudi **porast oglasov, ki vodijo neposredno v spletno zlorabo** – lažno trgovino, phishing spletno mesto, kripto prevaro ipd. Oglaševalske platforme, na primer Meta, Google Ads in oglaševalske mreže, so spletni napadalci popolnoma usvojili in so postale že del običajne poslovne prakse. Uporaba (oziroma natančneje zloraba) legitimnih oglaševalskih orodij za zavabljanje uporabnikov v različne spletne prevare ni novost, presenetljivo pa je, kako pogosti so postali tovrstni oglasi, kako dobro ciljajo uporabnike in kako malo vzvodov je na voljo, da bi se zaščitili spletni uporabniki.

1 LOKALIZACIJA
2 PERSONALIZACIJA
3 MOBILE FIRST
4 OGLAŠEVANJE PREVAR

NACIONALNI PROGRAM OZAVEŠČANJA O KIBERNETSKI VARNOSTI

VARNI NA INTERNETU

VARNI
NA INTERNETU
Od mene je odvisno vse.

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.

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

URSIV

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 ... Zaupanje v programske rešitve pred takšnimi zlorabami ne obvaruje – edina rešitev je kontinuirano izobraževanje spletnih uporabnikov.

KOGA NAGOVARJAMO?

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, delovno neaktivni prebivalci, ki niso več vpeti v formalne procese izobraževanja, hkrati pa niso deležni dodatnih izobraževanj o kibernetski varnosti.

ODRASLI UPORABNIKI

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.

ZAPOSLENI, SAMOZAPOSLENI, MANJŠA PODJETJA

KOMUNIKACIJSKI ŠTEVEC V LETU 2023

16 objavljenih opozoril in priporočil na spletni strani ***www.varninainternetu.si***

246 objav na naši Facebook strani

72 objav na Instagram strani in **607** story objav

10.284 prejemnikov e-novičnika Varne novice in 20 poslanih edicij do konca leta 2023

42.650 sledilcev na Facebooku in

3.526 sledilcev na Instagramu do konca leta

679 digitalnih zaslonov po vsej Sloveniji vključenih v širšo kampanjo Evropski mesec kibervarnosti

734 medijskih objav o programu Varni na internetu

5.158 izdanih certifikatov Varni v pisarni

31.000 natisnjenih priročnikov ABC varnosti na spletu.

NOVI NAGRADI ZA PROGRAM OZAVEŠČANJA

NAJBOLJŠI EVROPSKI VIDEO

Evropska agencija za kibernetsko varnost ENISA je podelila nagrade državam članicam za njihova gradiva, ki jih pripravijo v sklopu kampanje Evropski mesec kibernetske varnosti. **Že drugo leto zapored smo prejeli nagrado za najboljši video!** Tokrat za promocijski video za naš brezplačni spletni tečaj Varni v pisarni, s katerim smo nagovarjali predvsem vodstvo podjetij in IT-kader, da vlaga v izobraževanje svojih zaposlenih in tako pomembno zmanjša tveganja.

enisa
EUROPEAN UNION AGENCY FOR CYBERSECURITY

EUROPEAN CYBER SECURITY MONTH

EUROPEAN CYBERSECURITY MONTH
AWARDS CERTIFICATE

THE 2023 "BEST VIDEO" AWARD WAS AWARDED TO:

SLOVENIA

FOR THE MATERIAL "SAFE AT THE OFFICE"

Athens, 2023 October
The EU Agency for Cybersecurity
www.enisa.europa.eu
www.cybersecmonth.eu

NAJBOLJŠI STROKOVNI PRISPEVEK S PODROČJA VARNOSTI

Še posebej smo ponosni na nagrado, ki nam jo je podelil Inštitut za korporativne varnostne študije v sodelovanju s Slovenskim združenjem korporativne varnosti. Neodvisna komisija je naš program ozaveščanja Varni na internetu izbrala za prestižno nagrado Slovenian Grand Security Award 2023 v kategoriji Najboljši strokovni prispevek s področja varnosti. Gre za najbolj cenjeno nagrado s področja varnosti v Sloveniji, ki se podeljuje izbranim institucijam in posameznikom za njihov inovativni prispevek na področju razvoja in uveljavljanja varnosti.

KAJ JE ODMEVALO NA DRUŽBENIH OMREŽJIH?

Najodmevnejša objava na Facebook strani Varni na internetu v letu 2023 je bilo naše opozorilo o zavajajočem zapisu, s katerim naj bi se uporabniki obvarovali pred naročnino za uporabo Facebooka. Zapis, ki je obkrožil platformo, je bil neresničen, uporabniki pa so ga kljub temu množično delili. Naše opozorilo je doseglo več kot 16.700 interakcij, 2.228 odzivov in kar 1.500 delitev. Odmevnost objave se kaže tudi v 200 novih sledilcih na dan objave.

Na Instagramu je največ všečkov prejelo opozorilo o prevari z nagradno igro, v kateri naj bi uporabniki zadeli iPhone. Šlo je za prevaro s skrito naročnino, prevaranti pa so uporabnike označevali v svojih lažnih objavah.

V SREDIŠČE SMO POSTAVILI STAREJŠE UPORABNIKE

Vsako leto v središče izobraževalnih dejavnosti postavimo temo, ki jo zaznamo kot bolj perečo za določen del spletnih uporabnikov. Leta 2022 so bili to napadi na zaposlene v podjetjih, leta 2023 pa je bilo več dejavnosti v sklopu programa Varni na internetu posvečenih izobraževanju starejših. Eden izmed razlogov je opažen porast prijav incidentov, kjer so se po pomoč obračali otroci, katerih starši so nasedli na katero izmed spletnih prevar. Na drugi strani so se v zadnjih letih po pomoč vse pogosteje obračala različna društva in izobraževalne ustanove s prošnjo po izvedbi predavanja o spletni varnosti za starejše, saj so zaznali, da je ta populacija med ranljivejšimi. Starejši uporabniki spadajo v populacijo, starejšo od 65 let. To so večinoma upokojenci, delovno neaktivni prebivalci, ki niso več vpeti v formalne procese izobraževanja, hkrati pa niso deležni dodatnih izobraževanj o kibernetski varnosti, na primer v službi. Po podatkih Statističnega urada je trenutno to več kot 20 % vseh prebivalcev Slovenije, hkrati pa gre za delež prebivalstva, ki najhitreje narašča.

ŠIBKE DIGITALNE VEŠČINE STAREJŠIH

Tudi na SI-CERT smo skozi vsakodnevno komunikacijo s spletnimi uporabniki in obravnavo incidentov prepoznali določene tipe spletnih prevar, kjer so pogostejše žrtve starejši uporabniki. Razlogov, zakaj v določenih primerih starejši spletnih nevarnosti ne prepoznajo, je več. Na prvem mestu so gotovo šibke digitalne veščine starejših. Statistični urad je v raziskavi leta 2021 ugotovil, da je bil v Sloveniji delež oseb brez digitalnih veščin največji v starostni skupini 65–74 let, in sicer je znašal 45 %, kar je nad povprečjem EU-27 (41 %). Na SI-CERT opažamo tudi druge značilnosti, na primer starejši bolj zaupajo uradnim institucijam (policija, FURS, banke ipd.) in se jim zdi nepredstavljivo, da nekdo upa zlorabiti njihovo podobo, na primer ime, logotip, grb, in se predstavljati v njihovem imenu. Posledično so bolj izpostavljeni smishing in phishing prevaram, kjer napadalci ribarijo za gesli in finančnimi podatki ravno pod krinko znanih podjetij in institucij. Vsi ti dejavniki prispevajo k temu, da spletni napadalci preprosteje najdejo svoje žrtve med starejšimi uporabniki.

SPLETNE PREVARE, KI MERIJO NA STAREJŠE UPORABNIKE

Na SI-CERT smo skozi prakso identificirali spletne prevare, ki so jim bolj izpostavljeni starejši. Na prvem mestu so gotovo **ljubezenske prevare**, kjer so žrtve v večini obravnavanih primerov starejše vdove. To je tudi prevara, kjer se po pomoč največkrat obrnejo svojci žrtve. V nemalo primerih žrtve izgubijo vse življenjske prihranke, pa tudi nepremičnine. Vse več je tudi prijav glede **oglaševanja čudežnih zdravil in medicinskih pripomočkov**, ki obljubljajo povrnitev sluha, odpravo revme in drugih zdravstvenih težav. Nemalokrat so v oglasih uporabljene fotografije in imena slovenskih zdravnikov, vendar gre za zlorabo njihove identitete.

Gre za problematiko, ki ne spada v področje kibernetske varnosti, vendar smo javnost večkrat opozorili na zavajajoče oglase in problematiko naslovili na več inšpekcijskih služb. Vprašanji, kdo je odgovoren za zavajajoče oglase (oglaševalec, oglaševalska mreža ali ponudnik oglasnega prostora) in kdo je pristojen za sankcioniranje kršitev, ostajata neodgovorjeni. Pristojnosti nadzornih organov so omejene, saj naročniki oglasov niso podjetja s sedežem v Sloveniji. Oglaševalske mreže prav tako ne, hkrati pa celotno odgovornost za vsebino oglasov prelagajo izključno na naročnika oziroma oglaševalca. Podoben odziv je tudi pri ponudnikih medijskega prostora, ki prav tako ne odgovarjajo za vsebino oglasov, ki se pojavljajo v njihovem inventarju.

Izpostavljene so še različne **obljube o spletnih kreditih in možnosti dela od doma z velikimi zaslužki**. Gre za prevare, v katerih ljudje izgubijo vse, kar so dolga leta skrbno varčevali. **Veliko preplaha med starejšimi uporabniki povzročijo tudi lažne grožnje v imenu policije.** Taka elektronska sporočila so poslana na veliko naključnih naslovov. Cilj goljufov je najti nekaj posameznikov, ki jih bodo navedbe dovolj prestrašile, da bodo na sporočilo odgovorili, čeprav so vse navedbe popolnoma izmišljene.

EVROPSKI MESEC KIBERNETSKE VARNOSTI

Tudi kampanjo Evropski mesec kibervarnosti smo posvetili starejšim uporabnikom. **Oktobra smo izvedli oglaševalsko kampanjo, v katero so bili vključeni digitalni zasloni v mestnih avtobusih v Ljubljani, Mariboru in Celju, v 179 nakupovalnih središčih po vsej Sloveniji in na zaslonih v središču Ljubljane.** V medijski plan smo tako vključili zaslone na mestih, kjer bi kar najbolj ciljano dosegli populacijo starejših. **Zasnovali smo serijo animiranih videov, ki opozarjajo na najpogostejše spletne prevare, predstavljene skozi pogled pametnih telefonov**. Ti postajajo vse pogostejši vektor napadov spletnih goljufov. Animacije prikazujejo različne situacije, v katerih se lahko znajde slehernik, ko prejme na prvi pogled povsem običajno SMS-sporočilo, ki pa skriva poskus ribarjenja za podatki, kripto investicijske prevare oziroma lažno nagradno igro.

Animacije o spletnih prevarah so na videozaslonih predvajali tudi v poslovalnicah Pošte Slovenije, kjer so se odzvali naši prošnji k sodelovanju in omogočili brezplačno predvajanje.

Vse dejavnosti smo predstavili na **novinarski konferenci, ki smo jo organizirali v sodelovanju z Ministrstvom za digitalno preobrazbo**, kjer prav tako izvajajo programe krepitve digitalnih veščin starejših. Naš cilj je bil predstaviti konkretne rešitve in učna gradiva, ki smo jih zasnovali in tako še okrepili zavedanje javnosti o tej problematiki ter predvsem usmerili, kje lahko dobijo potrebno pomoč.

EVROPSKI MESEC KIBERNETSKE VARNOSTI

DEJAVNOSTI NA DRUŽBENIH OMREŽJIH

Kampanja ozaveščanja v okviru meseca kibervarnosti je potekala tudi na družbenih omrežjih Facebook in Instagram, kjer smo z zelo omejenim proračunom za oglaševanje dosegli veliko uporabnikov, kar 160.000. Z oglasi smo ciljali dve skupini, in sicer uporabnike do 50 let in starejše od 65 let. Pri tem smo želeli doseči čim več uporabnikov in jih opozoriti na najpogostejše prevare, ki ciljajo na starejše, ter jim podati informacije o tem, kje lahko poiščejo pomoč. Poleg oglasov v obliki tematskih animacij smo vsak dan objavljali tudi organske objave, katerih rdeča nit je bil družbeni inženiring. Tudi tokrat je za večino materialov poskrbela Agencija EU za kibernetsko varnost ENISA, mi pa smo jih prevedli in priredili za slovenski prostor. Ob tem smo, kot vedno, ozaveščali tudi o aktualnih prevarah in lastne materiale smiselno povezali ter umestili v skupni koledar objav v oktobru. Z organskimi objavami smo v tem obdobju dosegli 168.000 uporabnikov na Facebooku in 43.000 na Instagramu.

OSREDOTOČENJE NA ZAPOSLENE – NE NAJŠIBKEJŠI, AMPAK SPREGLEDAN ČLEN

Pomemben, a pogosto spregledan dejavnik, ki prispeva k varnosti celotne organizacije, je tudi opolnomočen zaposleni, ki se zaveda pomembnosti varovanja podatkov in zaščite naprav. Zaposleni so popolnoma 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 oziroma socialnega inženiringa. 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 uporabnikov. Na SI-CERT-u že leta opozarjamo, da je še vedno (pre)pogosto prepričanje, da manjša podjetja niso zanimiva za spletne napadalce, kar pa ne drži. Če zaposleni nimajo ustreznih znanj in veščin, da bi prepoznali nevarnost, so napadalci pogosto uspešni.

Zato je spletni tečaj Varni v pisarni še ena od izobraževalnih dejavnosti, ki se izvajajo v okviru programa Varni na internetu. Platforma, ki temelji na videopredavanjih, na preprost, razumljiv in vizualno privlačen način zaposlenim predstavi osnove informacijske varnosti. Spletni tečaj je brezplačen, poteka kadarkoli na zahtevo, prilagojen je različnim delovnim mestom, osnovni modul pa vam bo vzel zgolj 30 minut. Učne teme so razdeljene na module in prilagojene različnim delovnim procesom (splošne vsebine za vse zaposlene, za računovodje in poslovne sekretarje, za marketing in nabavo ter za IT-kader), zato je tečaj primeren tudi za vse organizacije, kjer ni sistematičnega pristopa k izobraževanju o informacijski varnosti.

Brezplačni spletni tečaj Varni v pisarni, namenjen usposabljanju zaposlenih o informacijski varnosti, je od postavitve platforme leta 2021 do konca leta 2023 izobrazil 9053 tečajnikov, ki so skupaj opravili skoraj 16.000 izobraževalnih modulov.

Spletni tečaj Varni v pisarni je brezplačen, poteka kadarkoli na zahtevo, traja 30 minut in je prilagojen različnim delovnim mestom v organizaciji. Na naslovu www.varnivpisarni.si lahko vsakdo opravi registracijo in začne s tečajem v lastnem tempu ter izbere vsebine, povezane z delovnim mestom.

Vsebine tečaja so s podpisom sporazuma v 2023 umeščene tudi v e-usposobljanje Informacijska varnost, ki ga izvaja Upravna akademija pri Ministrstvu za javno upravo. S prikazom dobrih praks zaščite informacijskih sredstev in podatkov tako v kot izven pisarne, prispevamo k razvoju digitalnih veščin javnih uslužbencev.

Naslov publikacije: **Poročilo o kibernetski varnosti za leto 2023**
Avtor publikacije: **Nacionalni odzivni center za kibernetsko varnost SI-CERT**
Leto izida: **2024**
Naklada: **550 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