SPOROČILO ZA JAVNOST, ZA TAKOJŠNJO OBJAVO

Letno poročilo o kibernetski varnosti 2021

Kibernetska varnost je v času pospešene digitalizacije ključnega pomena

Ljubljana, 25. avgust 2022

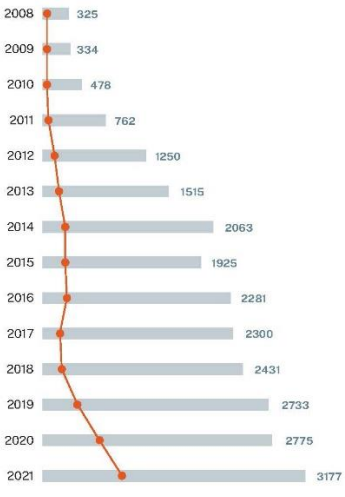
Nacionalni odzivni center za kibernetsko varnost SI-CERT je izdal Poročilo o kibernetski varnosti za leto 2021. Zabeleženih je bilo 3177 incidentov, kar predstavlja 14,49 % povečanje v primerjavi z letom prej. Med incidenti so ponovno izstopali phishing napadi, ki so predstavljali skoraj tretjino vseh prijav, ter podtikanje škodljive kode. Leto 2021 je najbolj zaznamovalo veliko število razkritih ranljivosti, pri čemer so bile v ospredju ranljivosti dobavne verige.

Phishing še vedno najpogostejša prevara

V letu 2021 so na SI-CERT skupno obravnavali 3177 incidentov, med katerimi so tako kot zadnja leta prednjačili phishing napadi. Ti so se v primerjavi z letom 2020 povečali za skoraj 37 %, skupno pa so predstavljali skoraj tretjino vseh prejetih prijav. Čeprav gre za eno najstarejših vrst spletnih napadov, ki so tehnično zelo enostavni, so še vedno relativno uspešni.

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

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



Slika 1: Število incidentov v letih 2008-2021, SI-CERT

Velik delež incidentov je predstavljala tudi zlonamerna koda - **trojanski konji, ki okužijo vaš računalnik in vam ukradejo shranjena gesla in digitalna potrdila.** Ti se najpogosteje širijo prek priponk in običajno predstavljajo prvi korak pri nepooblaščenem dostopu do omrežja podjetja prek okužbe računalnika zaposlenega. Druga vrsta nevarne zlonamerne kode so še vedno **izsiljevalski virusi**, pri čemer kibernetski kriminalci ciljajo podjetja. Podjetja so namreč za odšifriranje datotek praviloma pripravljena plačati več kot posamezniki, domači uporabniki – zahtevane odkupnine se lahko gibljejo tudi do več milijonov evrov.

Oškodovanja vse višja, povprečna izguba pri kripto prevarah kar 28.000 evrov

Ob prijavi incidenta SI-CERT beleži tudi neposredna oškodovanja, a le na podlagi prostovoljne priglasitve prijavitelja. Skupaj je bilo v letu 2021 zabeleženih 166 oškodovanj, kar predstavlja le nekaj več kot 5 % vseh obravnavanih incidentov. Vendar je skupen znesek finančne škode pri omenjenih incidentih znašal kar 1,45 milijonov evrov. Najvišje oškodovanje, nekaj več kot 123.000 evrov, so zabeležili pri vrivanju v poslovno komunikacijo (ang. business e-mail compromise). Vse višja oškodovanja opažajo tudi pri investicijskih prevarah v kriptovalute – najvišje zabeleženo oškodovanje v lanskem letu je znašalo 100.000 evrov, medtem ko se je povprečen znesek izgubljenega vložka gibal okoli 28.000 evrov.

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

Slika 2: Povprečna oškodovanja glede na vrsto zlorabe, SI-CERT, Poročilo o kibernetski varnosti 2021

Leto ranljivosti dobavne verige

Zagotovo pa so leto 2021 zaznamovale številne varnostne ranljivosti, ki so tekom leta zaposlovale celotno skupnost odzivnih centrov za kibernetsko varnost (znanih tudi pod kratico CSIRT, Computer Security Incident Response Team). V ospredju so bile predvsem ranljivosti dobavne verige (ang. supply chain). Niz se je pričel že marca 2020 z vdorom v omrežje proizvajalca SolarWinds, do razkritja katerega pa je prišlo šele proti koncu leta. Nekaj mesecev kasneje je sledila prva v seriji ranljivosti strežnikov Microsoft Exchange, do konca leta pa so se zvrstile še ranljivosti ProxyShell, poštnega strežnika Exim in Kaseya. Leto se je zaključilo v stanju povečane pripravljenosti celotne mreže odzivnih centrov CSIRT Evropske unije zaradi 0-day ranljivosti v knjižnici Log4J. Veliko število ranljivosti je izpostavilo pomen skrbi za celoten ekosistem kibernetskega prostora, še posebno pri pospešeni digitalizaciji, ki smo ji priča v zadnjih letih.

Kako se zaščititi?

Nacionalni odzivni center za kibernetsko varnost SI-CERT redno obvešča javnost prek novičnikov Odziv in Varne novice. Prvi je namenjen strokovni javnosti, drugi pa ozavešča o trenutno najbolj aktualnih spletnih goljufijah, ki so jim izpostavljeni posamezniki in podjetja. Napotke za zaščito in zmanjšanje tveganj pri uporabi spleta SI-CERT deli tudi prek svojih kanalov na družbenih omrežjih in na spletnih straneh cert.si ter varninainternetu.si. Ker vse več prevar cilja na podjetja, so na SI-

CERT za zaposlene zasnovali tudi brezplačni spletni tečaj Varni v pisarni, ki podaja pomembna znanja za zagotavljanje kibernetske varnosti v poslovnem okolju.

OPOMBE ZA UREDNIKE

Nacionalni odzivni center za kibernetsko varnost SI-CERT (*Slovenian Computer Emergency Response Team*) opravlja koordinacijo razreševanja incidentov, tehnično svetovanje ob vdorih, računalniških okužbah in drugih zlorabah ter izdaja opozorila za upravitelje omrežij in širšo javnost o trenutnih grožnjah. SI-CERT izvaja nacionalni program ozaveščanja Varni na internetu. Delovanje centra SI-CERT je opredeljeno v 28. členu Zakona o informacijski varnosti.

Za vse dodatne informacije smo vam na voljo.

press@cert.si