REPUBLIKA SLOVENIJA
URAD VLADE REPUBLIKE SLOVENIJE
ZA INFORMACIJSKO VARNOST

URSIV

Polletno poročilo o kibernetskih incidentih 2024-1

Oktober 2024

UVOD

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je kot pristojni nacionalni organ za informacijsko varnost med drugim odgovoren za vzpostavitev in delovanje nacionalnega sistema zagotavljanja kibernetske varnosti ter za njegovo koordinacijo v Republiki Sloveniji. Poleg tega izvaja naloge enotne kontaktne točke za zagotavljanje čezmejnega sodelovanja z ustreznimi organi drugih držav članic EU in z evropsko mrežo skupin za obravnavo incidentov s področja varnosti elektronskih omrežij in informacij (CSIRT).

V skladu s šestim odstavkom 25. člena Zakona o informacijski varnosti (Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23, v nadaljevanju ZInfV) URSIV dvakrat letno pripravi poročilo o varnostnih dogodkih[1] in incidentih[2] kibernetske varnosti v Republiki Sloveniji. Namen poročila je seznanjanje javnosti o aktualnem stanju kibernetske varnosti v državi. Posledično predstavlja sintezo aktualnih statističnih podatkov za obdobje zadnjega pol leta, kot tudi primerjalno analizo kibernetskih dogodkov, incidentov in aktivnosti v kratkoročnem preteklem obdobju. Hkrati pa na podlagi preteklih trendov in specifike kibernetskih incidentov poda priporočila glede ukrepov, s katerimi lahko organi na državni in lokalni ravni ter drugi subjekti poskrbijo za boljšo kibernetsko varnost njih samih.

Poročilo je pripravljeno na podlagi podatkov in informacij pridobljenih s strani SI-CERT *(angl. Slovenian Computer Emergency Response Team)*, ki je pristojni nacionalni odzivni center za kibernetsko varnost za zavezance - izvajalce bistvenih storitev (v nadaljevanju: IBS) iz sektorjev energija, digitalna infrastruktura, oskrba s pitno vodo in njena distribucija, zdravstvo, promet, bančništvo, infrastruktura finančnega trga, preskrba s hrano in varstvo okolja ter ponudniki digitalnih storitev.
Poleg tega poročilo vsebuje tudi podatke SIGOV-CERT, ki je pristojni odzivni center za incidente v informacijskih sistemih organov državne uprave (ODU) in povezanih subjektov. SIGOV-CERT je notranja organizacijska enota URSIV. Oba odzivna centra (imenovana tudi CSIRT[3]) se v skladu z zakonom odzivata tudi na prostovoljno priglašene dogodke in incidente.

OBRAVNAVA DOGODKOV IN INCIDENTOV V OBDOBJU OD JANUARJA DO JUNIJA 2024

V prvem polletju leta 2024 sta oba odzivna centra skupaj obravnavala 2589 varnostnih dogodkov in incidentov. V primerjavi s prejšnjim polletjem se je število priglašenih varnostnih dogodkov in incidentov povečalo[4]. Med priglašenimi dogodki in incidenti je bilo največ priglasitev izvedenih na podlagi prostovoljne priglasitve s strani fizičnih oseb in subjektov, ki niso zavezanci po Zakonu o informacijski varnosti, sledile pa so prijave s strani organov državne uprave. Poleg sektorja državne uprave, so bili najbolj izpostavljeni še energetski, izobraževalno-raziskovalni, bančni, prometni in zdravstveni sektor. Med prijavljenimi incidenti je bilo skupaj zabeleženih 13 težjih incidentov (oznaka C2 in C3), 1012 lažjih incidentov (oznaka C4 in C5) in 1534 varnostnih dogodkov (oznaka C6).

[1] Varnostni dogodek je vsaka zaznana kibernetska aktivnost, ki nima vpliva na omrežja in informacijske sisteme oziroma informacijske storitve zavezancev, ima pa lahko zaznan ali možen vpliv na posamezne fizične osebe ali posamezna podjetja v državi, ki niso zavezanci.

[2] Kibernetski incident je vsak dogodek, ki ima dejanski negativni učinek na varnost omrežij in informacijskih sistemov.

3 CSIRT – Computer Security Incident Response Team.

[4] V drugem polletju leta 2023 je bilo zabeleženih 1554 varnostnih dogodkov in incidentov.

Tabela 1: Število obravnavanih incidentov od 1. januarja do 30. junija 2024

Mesec	SI-CERT	SIGOV-CERT	Skupaj
Januar 2024	280	77	357
Februar 2024	282	62	344
Marec 2024	308	198	506
April 2024	265	224	489
Maj 2024	248	260	508
Junij 2024	193	192	385
SKUPAJ 1. polletje 2024	**1576**	**1013**	**2589**

Vir: SIGOV-CERT in SI-CERT

SI-CERT je v prvem polletju obravnaval skupaj 1576 varnostnih dogodkov in incidentov, kar pomeni precejšnje povečanje števila kot v drugem polletju leta 2023, ko jih je obravnavala 951. Od omenjenih je obravnaval 5 težjih incidentov z oznako C2 in C3, 19 lažjih incidentov z oznako C4 in C5 ter 1552 varnostnih dogodkov z oznako C6.

Tabela 2: Stopnje varnostnih dogodkov in incidentov

Oznaka	1. četrtletje	2. četrtletje	Skupaj
C1			
C2	1		1
C3	4		4
C4	6	9	15
C5	2	2	4
C6	857	695	1552
SKUPAJ	**870**	**706**	**1576**

Vir: SI-CERT

Med oblikami varnostnih dogodkov in kibernetskih incidentov prevladujejo različne oblike spletnih goljufij, katerih žrtve so predvsem fizične in druge pravne osebe, ki dogodke in incidente prijavljajo na podlagi prostovoljne prijave in niso zavezanci po ZInfV, kar je razvidno iz tabele 3.

Tabela 3: Kategorije in vrste incidentov

Kategorija	Vrsta	1. četrtletje 2024	2. četrtletje 2024
Neprimerna vsebina	Neželena sporočila	49	22
Neprimerna vsebina	Žaljiva vsebina	6	5
Neprimerna vsebina	Nasilna vsebina		1
Zlonamerna koda	Črv		
Zlonamerna koda	Virus	4	4
Zlonamerna koda	Trojanski konj	32	35
Zlonamerna koda	Vohunska programska oprema		1
Zlonamerna koda	Rootkit		

Zlonamerna koda	Boti in botneti	1	1
Zlonamerna koda	Nadzorni strežnik		
Zlonamerna koda	Izsiljevalski virus	10	8
Zlonamerna koda	Orodje za oddaljen nadzor (RAT)	11	5
Zbiranje informacij	Odkrivanje potencialnih tarč in ranljivosti (skeniranje)	3	5
Zbiranje informacij	Prestrezanje komunikacije		
Zbiranje informacij	Socialni inženiring	2	
Poskusi vdora	Izkoriščanje znane ranljivosti		
Poskusi vdora	Poskusi prijav, bruteforce in napadi s slovarjem	4	3
Vdor	Zloraba priviligiranega uporabniškega računa	2	
Vdor	Zloraba nepriviligiranega uporabniškega računa	37	41
Vdor	Napad na aplikacijo	2	**7**
Razpoložljivost	Napad onemogočanja	2	1
Razpoložljivost	Porazdeljen napad onemogočanja	10	25
Razpoložljivost	Izpad delovanja naprav ali omrežja	2	1
Varnost informacijskih virov	Nepooblaščen dostop do podatkov	1	5
Varnost informacijskih virov	Nepooblaščeno spreminjanje podatkov	5	5
Varnost informacijskih virov	Odtekanje informacij	1	2
Goljufije	Nepooblaščeno izkoriščanje virov	6	5
Goljufije	Intelektualna lastnina in avtorske pravice	5	2
Goljufije	Kraja identitete	27	11
Goljufije	Phishing sporočilo	50	19
Goljufije	Phishing spletno mesto	21	12
Goljufije	Spletno nakupovanje	90	46
Goljufije	Goljufija z vnaprejšnjim plačilom	32	19
Goljufije	Izsiljevanje	86	88
Goljufije	Druge goljufije	256	210
Ranljivosti	Odgovorno razkrivanje		3
Ranljivosti	Razkritje ranljivosti	4	2
Ranljivosti	Ranljivi sistemi in naprave	6	6
Drugo	Drugo	103	106
Test	Namenjeno testom		
SKUPAJ		**870**	**706**

Vir: SI-CERT

Kot že omenjeno, so bili med najbolj prizadetimi energetski, izobraževalno-raziskovalni, bančni, prometni in zdravstveni sektor, kar je razvidno iz spodnje tabele 4.

Tabela 4: Razdelitev po sektorjih

Skupina	Sektor	1. četrtletje	2. četrtletje	Skupaj
Ostalo	Fizična oseba	76	60	136
Ostalo	Druge pravne osebe	78	76	154
NIS	Bančništvo	7	4	11
Ostalo	Raziskovalno-izobraževalni sektor	14	17	31
Ostalo	Drugo	657	507	1164
ZInfV	Organi državne uprave	12	16	28
Ostalo	Operaterji elektronskih komunikacij	6	1	7
NIS	Zdravstvo	8	2	10
NIS	Promet	3	7	10
NIS	Energija	5	9	14
NIS	Digitalna infrastruktura	3	6	9
NIS	Ponudniki spletne tržnice	0	0	0
NIS	Oskrba s pitno vodo in distribucija	0	0	0
NIS	Ponudniki računalništva v oblaku	0	0	0
NIS	Infrastruktura finančnih trgov	1	1	2
Skupina		**1. četrtletje**	**2. četrtletje**	**Skupaj**
SKUPAJ		**870**	**706**	**1576**

Vir: SI-CERT

Iz tabele 5 so razvidne tudi neposredne finančne izgube prijaviteljev različnih varnostnih dogodkov in incidentov, ki jih je zabeležil SI-CERT. Največja zabeležena finančna izguba na področju goljufij je znašala 525.983,00 EUR. Ob tem tudi ostale finančne izgube niso zanemarljive in lahko predstavljajo veliko breme predvsem za manjša in srednje velika podjetja ter primerljive organizacije.

Tabela 5: Neposredna finančna izguba prijavitelja v EUR

Kategorija	3. četrtletje	4. četrtletje	Skupaj
Druge goljufije	62.850,00	463.133,00	525.983,00
Drugo	0	170,00	170,00
Goljufije z vnaprejšnjim plačilom	0	51,00	51,00
Izsiljevalski virus	5.000,00	0	5.000,00
Izsiljevanje	0	300,00	300,00
Nepooblaščeno izkoriščanje virov	0	669,00	669,00
Phishing sporočilo	500,00	87.012,00	87.512,00
Spletno nakupovanje	5.374,00	1.034,00	6.408,00
Trojanski konj	0	36.000,00	36.000,00
Zloraba neprivilegiranega uporabniškega računa	2.543,00	23.021,00	25.564,00
Orodje za oddaljen nadzor (RAT)	4.880,00	0	4.880,00
SKUPAJ	**81.147,00**	**611.390,00**	**692.537,00**

Vir: SI-CERT

SIGOV-CERT je v prvem polletju zaznal občutno povečanje priglašenih varnostnih dogodkov in kibernetskih incidentov, saj je skupno obravnaval 1013 varnostnih dogodkov in incidentov. V primerjavi s prejšnjim polletjem, je število poskočilo iz 603 na 1013. V omenjenem obdobju je obravnaval osem težjih incidentov z oznako C3, 993 lažjih incidentov z oznako C5 ter 12 varnostnih dogodkov z oznako C6. Največ priglašenih dogodkov in incidentov, in sicer 1004, je bilo na strani osrednje državne uprave, devet pa jih je bilo priglašenih s strani lokalne samouprave.

Tabela 6: Stopnje incidentov

Oznaka	3. četrtletje	4. četrtletje	Skupaj
C1			
C2			
C3	4	4	8
C4			0
C5	333	660	993
C6		12	12
SKUPAJ	337	676	1013

Vir: SIGOV-CERT

Zabeležene so bile različne oblike spletnih goljufij in spletnega ribarjenja, ki ostaja najpogostejša oblika priglašenega kibernetskega incidenta zadnjega polletja pri organih državne uprave. Zabeleženih je bilo tudi veliko število incidentov z uporabo zlonamerne kode in porast različnih oblik zbiranja informacij (skeniranja) ter drugih dogodkov kršitve informacijske varnosti, kar je razvidno iz tabele 7.

Tabela 7: Vrste dogodkov in incidentov

Vrsta	1. četrtletje	2. četrtletje	Skupaj
Žaljiva/zlonamerna vsebina	140	215	355
Goljufije	151	351	502
Zbiranje informacij	5	4	9
Informacijska varnost	13	65	78
Vdori/poizkusi vdora	4	0	4
Zlonamerna koda	2	15	17
Ranljivost	3	0	3
Razpoložljivost	3	12	15
Drugo	16	14	30
SKUPAJ	337	676	1013

Vir: SIGOV-CERT

Ranljivosti

Skupini CSIRT sta v prvi polovici leta objavili več opozoril o zaznanih ranljivostih. Ranljivost je obstoj šibkosti v arhitekturi informacijskega sistema ali omrežja, v varnostnih protokolih ali procesih, ali kot posledica napak v implementaciji ali upravljanju in je lahko izrabljena s strani zlonamernih akterjev (povzeto po ISO standardu[5]). Tako sta skupini v prvem četrtletju opozorili na dve pomembnejši

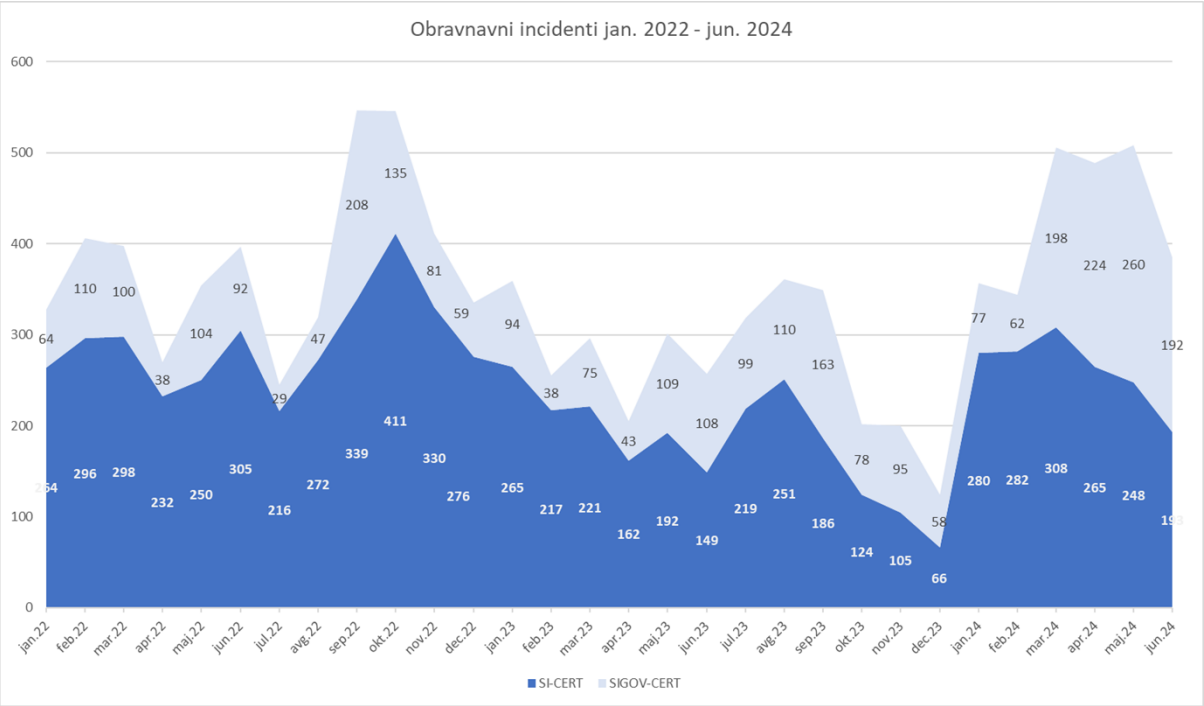
5 ISO/IEC TR 24772-1:2019(en), Programming languages — Guidance to avoiding vulnerabilities in programming languages — Part 1: Language-independent guidance.

ranljivosti, in sicer 0-day ranljivost v Ivanti Connect Secure VPN, ki omogoča neavtenticiranemu uporabniku izvajanje poljubnih ukazov na sistemu, in Fortinet kritično ranljivostih v sistemih FortiOS sslvpnd in fgfmd. Slednja omogoča oddaljenemu neavtenticiranemu akterju izvajanje poljubne kode na sistemu. Obe ranljivosti naj bi se tudi že izkoriščale z zlonamernih kibernetskih aktivnostih. Poleg tega se še vedno izkoriščajo že znane ranljivosti programske opreme, ki že imajo na voljo popravke. Razlog lahko leži v nedoslednem vzdrževanju informacijskih sistemov oz. programske opreme ter nedoslednega nameščanja popravkov. Pojavljajo se tudi tako imenovani »pozabljeni strežniki«. Vzroki so lahko v preobremenjenosti vzdrževalcev, neustreznem obvladovanju informacijskih sistemov in tudi malomarnosti oz. neodgovornem ravnanju.

OCENA

Statistični pregled števila priglašenih varnostnih dogodkov in kibernetskih incidentov kaže na porast, ob tem pa tudi na večjo raznolikosti.

Graf 1: Število obravnavanih incidentov od januarja 2022 do junija 2024



Vir: SI-CERT in SIGOV-CERT

V obravnavanem obdobju so med varnostnimi dogodki in kibernetskimi incidenti prevladovale različne oblike goljufij, predvsem je bilo veliko primerov spletnega ribarjenja (ang. Phishing) in uporabe zlonamerne programske opreme z izsiljevanjem (ang. Ransomware), ki predstavlja najpogostejše sredstvo storilcev kibernetske kriminalitete, ki so primarno finančno motivirani. Poleg omenjenih, je bilo statistično največ porazdeljenih napadov onemogočanja delovanja (ang. Distributed Denial of Service, DDoS), zlonamernih kibernetskih aktivnosti usmerjenih v pridobivanje podatkov, izvajanje socialnega inženiringa, uporabe zlonamerne programske opreme (ang. Malware), izkoriščanja ranljivosti v dobavnih verigah in groženj prek spleta. Poleg tega je v porastu tudi hektivizem, ki postaja vedno bolj nepredvidljiv. Zbrani podatki kažejo, da napadi postajajo vse bolj sofisticirani in kompleksni. Goljufi uporabljajo napredne tehnike socialnega inženiringa, da pridobijo zaupne informacije od žrtev. Zlonamerna elektronska sporočila in spletno ribarjenje so postali bolj ciljno usmerjeni in personalizirani, kar je povečalo njihovo učinkovitost. Pri tem jim pomaga vse hitreje razvijajoča tehnologija umetne inteligence in tehnologija za izdelavo kompleksnih ponaredkov (ang Deepfake), ki omogoča ustvarjanje zelo realističnih ponarejenih video vsebin.

Izkušnje iz prvega polletja leta 2024 so pokazale, da se geopolitične napetosti in oboroženi konflikti po svetu odražajo v kibernetskem prostoru Republike Slovenije. Predvsem hektivisične skupine so te situacije s pridom izkoriščale za doseganje svojih ciljev prek porazdeljenih napadov onemogočanja delovanja (DDoS). Gre za najbolj vidno, pogosto in medijsko izpostavljeno ter hkrati tudi najmanj nevarno obliko kibernetskega incidenta, ki se izkaže v nedelovanju spletnih strani. Kljub preprostosti in omejenim škodljivim posledicam jo hektivisti, oziroma hektivistične skupine uporabljajo kot orodje,

s katerim izražajo nestrinjanje z določenimi politikami in odločitvami vlad suverenih držav, mednarodnih podjetij in organizacij, s čimer tudi promovirajo svoje delovanje in ideologijo. Pro-ruske hektivistične skupine so tako v prvi polovici leta večkrat javno napovedale in tudi izvedle kampanjo DDoS napadov na spletne strani posameznih slovenskih državnih organov in podjetij, kot povračilni ukrep za slovensko podporo Ukrajini.

Tako so imele določene odločitve ali stališča Republike Slovenije, na primer vezane na podporo Ukrajini, neposredne implikacije na kibernetsko varnost Republike Slovenije. Skladno s tem in upoštevaje neprestano spreminjajoče se kibernetsko varnostno okolje, ki ga zaznamuje porast kibernetskih groženj in incidentov, se zahteva večja budnost in odzivnost.

Pridobljeni podatki iz prvega in delno drugega četrtletja tega leta kažejo na delni padec števila priglašenih incidentov s strani fizičnih oseb, s čimer lahko razumemo, da se je povprečni slovenski uporabnik informacijske tehnologije že prilagodil velikemu številu tovrstnih zlonamernih aktivnosti in jih rešuje samostojno, s tem, da sam prepreči negativne posledice. Na podlagi tega ocenjujemo, da se je izboljšala varnostna kultura in seznanjenost s splošnimi ukrepi za zagotavljanje kibernetske varnosti med državljani. Podoben napredek je, kljub porastu priglašenih varnostnih dogodkov in kibernetskih incidentov, opaziti tudi pri subjektih državne uprave.

Vse večjo nevarnost predstavljajo kibernetske aktivnosti, ki izkoriščajo ranljivosti v dobavni verigi in služijo kot vstopni vektor na primer za postavitev vohunske programske opreme ali pa kot vektor napada v primeru eskalacije že tako napetih odnosov med velikimi geopolitičnimi akterji. Gre za zelo pogosto obliko kibernetskega kriminala, za katero ocenjujemo, da bo tudi v prihodnje ostala ena izmed poglavitnih groženj za posameznike, podjetja državne organe in njihove poslovne ter delovne procese. Nenazadnje ima vse omenjeno tudi negativne učinke na varnost države.

URSIV je v sodelovanju z drugimi organi in mednarodnimi organizacijami pozorno spremljal situacijo na področju informacijske in kibernetske varnosti Republike Slovenije, v državah članicah Evropske unije ter širše. Med drugim je poleg rednih koordinacijskih in drugih aktivnosti na nacionalni ravni URSIV podpiral napore ozaveščanja ter krepitve informacijske in kibernetske varnosti v Republiki Sloveniji.

PREDLOGI IN PRIPOROČILA

Ob boku vse večjim geopolitičnim napetostim in porastu konfliktov po svetu, se soočamo tudi s splošnim povečanjem tako števila kot tudi raznolikosti kibernetskih dogodkov in incidentov. Njim so tako vse bolj izpostavljeni vsi uporabniki kibernetskega prostora. Pričakovati je, da se bo trend v tem, ali celo povečanem obsegu nadaljeval tudi v prihodnje.

Posledično predlagamo izvajanje aktivnosti za ohranjanje visokega nivoja kibernetske varnosti pri zavezancih, upoštevanje priporočil izdanih s strani URSIV, SIGOV-CERT in SI-CERT ter dosledno izpolnjevanje naloženih ukrepov za odpravo nepravilnosti in podanih priporočil, ki jih izda Inšpekcija za informacijsko varnost.

Predlagamo, da spremljate oziroma vaše sodelavce in tudi zunanje izvajalce opozorite na objave projekta Varni na internetu, ki ga izvaja SI-CERT (https://www.varninainternetu.si/) in projekta Center za varnejši internet, ki ga izvajajo Univerza v Ljubljani Fakulteta za družbene vede, Zavod Arnes, Zveza prijateljev mladine Slovenije in Zavod MISSS (www.safe.si/). SI-CERT je pripravil video serijo KLIK in brezplačni tečaj Varni v pisarni.

Vsem odgovornim za upravljanje informacijskih sistemov in omrežij priporočamo, da se v organizaciji:

- opravi popis procesov, določijo ključni procesi za delovanje in s tem povezana informacijska sredstva, ki te procese podpirajo;
- opravi popis informacijskih sredstev za namen zagotavljanja informacijske varnosti in izvede analiza tveganj informacijske varnosti;
- pripravijo in redno izvajajo ukrepi za obvladovanje identificiranih tveganj informacijske varnosti;
- preverijo implementirane varnostne mehanizme in nastavitve aplikacij, programov in informacijskih sistemov;
- preverijo varnostne nastavitve/ukrepe povezane z zmogljivostmi za delo od doma;
- redno posodabljajo programsko opremo. V primeru, da je omenjeno omejeno, pa naj se ustrezno zavaruje perimeter delovanja informacijskega sistema;
- vključijo uporabo več faktorske avtentikacije, kjer je to smiselno;
- dosledno izvajajo oceno tveganj in ukrepe za obvladovanje tveganj.

IBS, ODU, ponudnikom digitalnih storitev in povezanim subjektom ter ostalim podjetjem in ustanovam priporočamo, da:

- v pogodbe z zunanjimi izvajalci storitev in dobavitelji vključijo zahteve s področja zagotavljanja informacijske varnosti;
- dosledno skrbijo za ustrezen nivo varnostnega zavedanja zaposlenih in osnovne prakse kibernetske higiene ter izvajajo primerne aktivnosti za preprečitev notranjih groženj;
- implementirajo orodja za prepoznavo zlonamernih elektronskih sporočil;
- posvetijo dodatno pozornost neobičajnim ali povečanim kibernetskim aktivnostim znotraj svojih sistemov, ki bi lahko pomenile kibernetsko tveganje za njihovo delovanje;
- preverijo ukrepe za neprekinjeno delovanje oziroma zagotavljanje storitev;
- pregledajo postopke za zagotavljanje neprekinjenega poslovanja in postopke odzivanja na incidente;
- pregledajo podatke iz sistema za upravljanje varnostnih dogodkov in tveganj *(angl. Security Information and Event Manager, SIEM)* in drugih orodij ter opravijo analizo stanja (tip in obseg dogodkov) in v primeru kakršnih koli anomalij ustrezno postopajo.