Smjernice

za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga (u skladu sa Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga)

Verzija 3.0.

Ožujak 2023. godine

Sadržaj

Status

1. Ovaj dokument sadrži Smjernice za dostavu obavijesti o incidentima sa znatnim učinkom operatora ključnih usluga i davatelja digitalnih usluga na temelju članka 43. Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga. U skladu s odredbama Zakona o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (dalje u tekstu ZKS), isti su obvezni bez odgađanja izvijestiti nadležni CSIRT o incidentima sa znatnim učinkom.
2. Smjernice sadrže protokol izvješćivanja nadležnih CSIRT-ova, kriterije za definiranje znatnog učinka, obrasce izvješćivanja o incidentima te ostale ključne informacije za uspješnu komunikaciju operatora ključnih usluga i davatelja digitalnih usluga s nadležnim CSIRT-ovima.

Područje primjene i izuzeci

1. Ove Smjernice se primjenjuju na sve obveznike ZKS-a koji su tijekom procesa identifikacije (u skladu s člankom 7. ZKS) prepoznati kao operatori ključnih usluga ili davatelji digitalnih usluga.
2. Kako je navedeno u članku 21. ZKS, operatori ključnih usluga i davatelji digitalnih usluga dužni su nadležni CSIRT, bez neopravdane odgode, obavješćivati o incidentima koji imaju znatan učinak na kontinuitet usluga koje pružaju.
3. Kako je navedeno u Prilogu II ZKS-a, nadležni CSIRT-ovi su Zavod za sigurnost informacijskih sustava i Nacionalni CERT.
4. Procjena učinka incidenta provodi se korištenjem kriterija navedenih u Prilogu 1. ovih Smjernica.
5. **Incidenti koji nisu nastali kao posljedica izravnog kibernetičkog utjecaja na IT infrastrukturu (kibernetički napad, pogrešna konfiguracija i slično) već kao posljedica vanjskih neželjenih utjecaja (poplava, požar, krađa, elementarne nepogode) neće se primarno prijavljivati nadležnom CSIRT-u (CSIRT u ovom slučaju nije *first responder)*, već drugim nadležnim službama ovisno o prirodi incidenta. Korisnici će i u tom slučaju nadležnom CSIRT-u dostaviti inicijalnu obavijest, prijelazna i završno izvješće.**
6. Smjernice verzija 3.0 primjenjuju se od 10. ožujka 2023. godine.

Protokol dostave obavijesti o incidentima sa znatnim učinkom

1. U slučaju da ne postoji pouzdana poveznica između kriterija kojima se definira znatni učinak i (trenutnih) saznanja o učinku incidenta, korisnici trebaju pribjeći procjenama i temeljem istih odlučiti hoće li aktivirati protokol dostave obavijesti.
2. Nadležni CSIRT-ovi će informacije o incidentima te pripadajuća izvješća zaprimati putem PiXi platforme.[1]
3. Kod svakog operatora ključnih usluga ili davatelja digitalnih usluga određen je administrator na PiXi platformi koji ima ovlasti otvoriti nove korisničke račune unutar organizacije. Detalji korištenja PiXi platforme opisani su u korisničkim uputama dostavljenim svim korisnicima platforme.
4. Nakon popunjavanja ZKS incident obrasca na PiXi platformi, prijavu pregledava nadležni CSIRT definiran u Prilogu III ZKS-a. Ako je obrazac ispravno popunjen, nadležni CSIRT odobrava obrazac te se automatizirano obavještava Nadležno sektorsko tijelo. U slučaju prekograničnog učinka, automatizirano se obavještava i Jedinstvena nacionalna kontakt točka. Ako obrazac nije ispravno popunjen, prijavitelj od strane nadležnog CSIRT-a dobiva pojašnjenje razloga odbijanja prijave.

Inicijalna obavijest

1. Inicijalna obavijest o incidentu sa znatnim učinkom dostavlja se odmah, a najkasnije u roku od četiri sata od trenutka otkrivanja incidenta sa znatnim učinkom.
2. Podaci koji čine inicijalnu obavijest o incidentu sa znatnim učinkom nalaze se u obrascu u Prilogu 2. ovih Smjernica.
3. Nakon prijave inicijalne obavijesti na PiXi platformu, sustav omogućava prijavu prijelaznog izvješća.

Prijelazna izvješća

1. Do okončanja incidenta korisnik će nadležnom CSIRT-u informacije dostavljati i putem prijelaznih izvješća koja je potrebno nadopunjavati u skladu s novim saznanjima korisnika.
2. Prvo prijelazno izvješće o incidentu sa znatnim učinkom dostavlja se najkasnije u roku od tri radna dana od podnošenja inicijalne obavijesti o incidentu. Prijavitelj će putem PiXi platforme biti obaviješten o točnim rokovima za prijavu prijelaznog izvješća.

[1] PiXi platforma: nacionalna platforma za prikupljanje, analizu i razmjenu podataka o računalno-sigurnosnim prijetnjama i incidentima.

3. Korisnik će, bez odgode, dostavljati i dodatna prijelazna izvješća o incidentu sa znatnim učinkom ako sazna za nove podatke ili značajnije promjene do kojih je došlo od prvog prijelaznog izvješća, a osobito ako je incident eskalirao ili se smanjio, ako su otkriveni novi uzroci ili ako su poduzete nove radnje za rješavanje incidenta.
4. Protokol dostave prijelaznog izvješća bit će predočen nakon identifikacije operatora ključnih usluga i davatelja digitalnih usluga.
5. Nakon prijave prijelaznog izvješća u PiXi platformu sa statusom „Završen ZKS incident", sustav omogućava prijavu završnog izvješća.
6. Podaci koji čine prijelazno izvješće nalaze se u obrascu u Prilogu 3. ovih Smjernica.

Završno izvješće

1. Korisnici su dužni podnijeti završno izvješće o incidentu sa znatnim učinkom najkasnije u roku od 15 dana od dana procjene da je redovito pružanje usluge ponovno uspostavljeno. Prijavitelj će putem PiXi platforme biti obaviješten o točnim rokovima za prijavu završnog izvješća.
2. Protokol dostave završnog izvješća bit će predočen nakon identifikacije operatora ključnih usluga i davatelja digitalnih usluga.
3. Podaci koji čine završno izvješće nalaze se u obrascu u Prilogu 4. ovih Smjernica.

Komunikacija tijekom trajanja incidenta

1. Inicijalno, prijelazna i završno izvješće predstavljaju obvezni dio komunikacije između korisnika i nadležnog CSIRT-a u procesu rješavanja incidenta sa znatnim učinkom.
2. Tijekom trajanja incidenta korisnik i CSIRT uspostavit će neposredne kanale komunikacije (PiXi platforma, telefon, e-mail) za razmjenu svih operativnih informacija i podataka (npr. uzorci zlonamjernih programa, uzorak mrežnog prometa) neovisno o ovim Smjernicama definiranim izvješćima.
3. U slučaju nedostupnosti PiXi platforme, neovisno o razlogu, koristit će se alternativni načini komunikacije:
   - Nacionalni CERT:
     - Informacije o incidentu prijavljuju se na telefonski broj 01 6661 650 radnim danom između 9 i 16 sati te na broj 099 493 2091 izvan radnog vremena prema uputama opisanim na www.cert.hr/zks-incident
     - Inicijalne obavijesti, prijelazna i završna izvješća šalju se na e-mail adresu zks-incident@cert.hr
     - Obrasci za prijavu ZKS incidenta u slučaju nedostupnosti PiXi platforme nalaze se na www.cert.hr/zks-incident

- Zavod za sigurnost informacijskih sustava:
    - Informacije o incidentu na telefonski broj 01 4694 144 prema uputama opisanim na www.zsis.hr
    - Inicijalne obavijesti, prijelazna i završna izvješća šalju se na e-mail adresu cert@zsis.hr
    - Obrasci za prijavu ZKS incidenta u slučaju nedostupnosti PiXi platforme nalaze se na www.zsis.hr/default.aspx?id=405

4. U slučaju nedostupnosti PiXi platforme, neovisno o razlogu, korisnik je dužan ispuniti potrebne obrasce na platformi čim ona postane ponovno dostupna. Obrasce je potrebno ispuniti na PiXi platformi bez obzira na to jesu li isti ranije dostavljeni alternativnim načinom komunikacije opisanim u točki 3.

Prilog 1. Kriteriji za prepoznavanje znatnog učinka

Sektor	Podsektor	Ključna usluga	Kriteriji	Pragovi
Energetika	Električna energija	**Proizvodnja električne energije**	Smanjenje proizvodnje	60 MW
		Prijenos električne energije	Prekid prijenosa	Bez iznimke
		Distribucija električne energije	Prekid napajanja	Više od 20.000 obračunskih mjernih mjesta
	Nafta	**Transport nafte naftovodima**	Prekid transporta	Bez iznimke
		Proizvodnja nafte	Smanjenje proizvodnje naftnog polja	10.000 t/god
		Proizvodnja naftnih derivata	Smanjenje proizvodnje naftnih derivata	Motorni benzini: 40.000 t/god Dizelsko gorivo: 40.000 t/god Plinska ulja: 20.000 t/god
		Skladištenje nafte i naftnih derivata	Smanjenje skladišnog kapaciteta nafte na terminalu	200.000 m^3
			Smanjenje skladišnog kapacitet naftnih derivata pojedinog skladišta	12.000 m^3
	Plin	**Distribucija plina**	Prekid distribucije krajnjim kupcima	Više od 20.000 obračunskih mjernih mjesta
		Transport plina	Prekid transporta	Bez iznimke
		Skladištenje plina	Smanjenje skladišnih kapaciteta	5% potrošnje plina u RH u prethodnoj godini
		Prihvat i otprema UPP-a	Smanjenje kapaciteta uplinjavanja UPP u m^3/h	Više od 100.000 m^3/h
		Proizvodnja prirodnog plina	Smanjenje proizvodnje plina predanog u transportni sustav na pojedinom ulazu	20%
Prijevoz	Zračni promet	**Zračni prijevoz putnika i tereta**	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
		Upravljanje infrastrukturom zračne luke, uključujući upravljanje pomoćnim objektima zračne luke	Broj putnika pogođenih incidentom na pojedinoj zračnoj luci	20% od uobičajenog prometa
		Kontrola zračnog prometa	Narušavanje integriteta podataka na ključnim operativnim sustavima	Ugrožen jedan zrakoplov u bilo kojem volumenu kontroliranog zračnog prostora i na manevarskim površinama aerodroma
			Gubitak podataka na ključnim operativnim sustavima	Ugrožen jedan zrakoplov u bilo kojem volumenu kontroliranog zračnog

				prostora i na manevarskim površinama aerodroma
	Željeznički promet	**Upravljanje i održavanje željezničke infrastrukture, uključujući upravljanje prometom i prometno-upravljačkim i signalno-sigurnosnim podsustavom**	Ugrožavanje integriteta prometno-upravljačkog, signalno-sigurnosnog ili elektro-energetskog podsustava	Bez iznimke
		Usluge prijevoza robe i/ili putnika željeznicom	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
		Upravljanje uslužnim objektima i pružanje usluga u uslužnim objektima	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
		Pružanje dodatnih usluga koje su nužne za pružanje usluga prijevoza robe ili putnika željeznicom	Broj voznih jedinica (vlakova) pogođenih incidentom	10 dnevno
	Vodni prijevoz	**Nadzor kretanja brodova (VTS usluga)**	Ugrožavanje integriteta sustava za nadzor i upravljanje pomorskim prometom VTMIS i pružanja VTS usluga	Onemogućeno korištenje punih funkcionalnosti sustava za nadzor i upravljanje pomorskim prometom VTMIS i pružanja VTS usluga iz najmanje jednog kontrolnog centra u trajanju dužem od 3 sata
		Obavljanje poslova pomorske radijske službe	Ugrožavanje integriteta sustava pomorske radijske službe i pružanja usluga pomorske radijske službe	Onemogućeno korištenje punih funkcionalnosti sustava pomorske radijske službe i pružanja usluga pomorske radijske službe iz najmanje jedne obalne radijske postaje u trajanju dužem od 3 sata
		Održavanje objekata pomorske signalizacije	Ugrožavanje integriteta objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe	Nedostupnost najmanje 20% objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe u pojedinom plovnom području u trajanju dužem od 3 sata
				Nedostupnost najmanje 20% objekata pomorske signalizacije 1. kategorije značaja po sigurnost plovidbe u lukama otvorenim za javni promet od osobitog (međunarodnog) gospodarskog značaja za RH s prilaznim plovnim putovima u trajanju dužem od 3 sata

		Prijevoz putnika u međunarodnom i/ili domaćem prometu	Ovisnost drugih sektora o usluzi	Svi sektori čiji korisnici ili zaposlenici koriste pomorski prijevoz
			Utjecaj incidenata na gospodarske i društvene aktivnosti te na javnu sigurnost	Trajanje incidenta u periodu duljem od jednog dana
	Vodni prijevoz	**Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu**	Nedostupnost i ograničenost operativnog sustava	Nemogućnost obavljanja lučkih operacija u periodu duljem od 3 dana
			Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od 3 dana može uzrokovati zastoje u ovisnim sektorima
			Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od 3 dana može uzrokovati zastoje u ovisnim sektorima
		Prijevoz putnika, tereta i vozila u unutarnjim morskim vodama i teritorijalnom moru Republike Hrvatske koji se obavlja na unaprijed utvrđenim linijama prema javno objavljenim uvjetima reda plovidbe i cjenikom usluga	Onemogućeno obavljanje usluge prijevoza	Prekid obavljanja usluge prijevoza na više od 30% linija u trajanju duljem od 3 sata
		Praćenje i lociranje plovila u unutarnjoj plovidbi	Onemogućavanje rada „RIS“ sustava koji se odnosi na „Praćenje i lociranje plovila u unutarnjoj plovidbi“ (VTT)	Ugroza praćenja i lociranja minimalno jednog plovila u unutarnjoj plovidbi
		Obavijesti brodarstvu u unutarnjoj plovidbi	Onemogućavanje točne i pravovremene objave „Obavijesti brodarstvu u unutarnjoj plovidbi“	Ugroza objave minimalno jedne „Obavijesti brodarstvu u unutarnjoj plovidbi“
		Pristup elektroničkim navigacijskim kartama u unutarnjoj plovidbi	Onemogućenje rada korisničkih radnih stanica na obali u pristupu ćelijama „Elektroničkih navigacijskih karata u unutarnjoj plovidbi“ (ENC)	Onemogućeno korištenje minimalno jedne ćelije ENC-a
		Baza podataka o trupu plovila u unutarnjoj plovidbi	Ugroza točnosti sadržaja u bazi podataka	Ugroza sadržaja u bazi podataka za minimalno jedno plovilo
		Međunarodno elektroničko izvještavanje u unutarnjoj plovidbi	Nemogućnost primanja i slanja ERI poruka	Nemogućnost primanja/slanja minimalno jedne ERI poruke
	Cestovni prijevoz	**Javni prijevoz putnika**	Broj voznih jedinica pogođenih incidentom	20

			Broj putnika pogođenih incidentom	10.000
		Korištenje cestovne infrastrukture	Ugrožavanje integriteta prometno-upravljačkog, elektro-energetskog ili sustava za zaštitu od požara na cestovnoj infrastrukturi (uključujući objekte: mostovi, tuneli, vijadukti)	Bez iznimke
		Upravljanje prometnim tokovima ili informiranje vozača (ITS)	Prekid usluge centra za kontrolu i upravljanje prometom	30 minuta
			Prekid usluge centra za informiranje vozača o stanju u prometu	60 minuta
			Broj prometnih svjetala (semafora) pogođenih incidentom	10
Bankarstvo		**Platne usluge**	Kriteriji koje operatori ključnih usluga u sektoru bankarstva trebaju upotrijebiti za klasifikaciju značajnih operativnih ili sigurnosnih incidenata prema smjernicama Europskog nadzornog tijela za bankarstvo (EBA) iz članka 96. stavka 3. Direktive (EU) 2015/2366 o platnim uslugama na unutarnjem tržištu (PSD2 Direktiva)	Pragovi koje operatori ključnih usluga u sektoru bankarstva trebaju upotrijebiti za klasifikaciju značajnih operativnih ili sigurnosnih incidenata prema smjernicama Europskog nadzornog tijela za bankarstvo (EBA) iz članka 96. stavka 3. PSD2 Direktive
Infrastrukture financijskog tržišta		**Usluge mjesta trgovanja**	Trajanje incidenta	30 minuta
		Usluge središnjih drugih ugovornih strana (CCP)	Trajanje incidenta	30 minuta
Zdravstveni sektor		**Primarna zdravstvena zaštita**	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati
			Nedostupnost informacijskog sustava hitne medicinske pomoći	8 sati
		Sekundarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati

			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati
			Nedostupnost bolničkog informacijskog sustava u općoj bolnici	1 sat
		Tercijarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost bolničkog informacijskog sustava u kliničkom bolničkom centru	1 sat
			Nedostupnost bolničkog informacijskog sustava u kliničkoj bolnici	1 sat
			Nedostupnost bolničkog informacijskog sustava u klinici	1 sat
		Transfuzijska medicina i transplantacija organa	Nedostupnost informacijskog sustava za djelatnost transfuzijske medicine	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
			Nedostupnost koordinatora Nacionalnog transplantacijskog programa	1 sat
		Zdravstveno osiguranje i prekogranična zdravstvena zaštita	Nedostupnost informacijskog sustava ZOROH – Zdravstveno osiguranje – registar osiguranika Hrvatske	24 sata
			Nedostupnost servisa za provjeru statusa obveznog i dopunskog zdravstvenog osiguranja	8 sati
			Nedostupnost sustava za izdavanje Europskih kartica zdravstvenog osiguranja	72 sata
		Sigurnost hrane	Nedostupnost Središnjeg informacijskog sustava sanitarne inspekcije	24 sata

		Zaštita od opasnih kemikalija	Nedostupnost Registra sigurnosno-tehničkih listova	72 sata
			Nedostupnost Registra opasnih kemikalija proizvedenih ili uvezenih/unesenih na teritorij RH	72 sata
		Distribucija i sigurnost lijekova i medicinskih proizvoda	Nemogućnost obustave stavljanja u promet lijekova i povlačenja lijekova iz prometa	72 sata
			Nemogućnost praćenja ozbiljnih nesukladnosti i provjere kakvoće lijekova na tržištu RH	60 sati
			Nemogućnost praćenja sigurnosti medicinskih proizvoda	84 sata
		Nadzor nad zaraznim bolestima te skladištenjem i distribucijom cjepiva	Nedostupnost Nacionalnog javnozdravstvenog informacijskog sustava	8 sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	8 sati
Opskrba vodom za piće i njezina distribucija		**Opskrba krajnjih korisnika**	Prekid opskrbe zdravstveno ispravne vode iz sustava javne vodoopskrbe	više od 24 sata
			Potpuni prekid opskrbe vodom iz sustava javne vodoopskrbe	više od 24 sata
Digitalna infrastruktura		**DNS usluga za .hr TLD**	Nedostupnost usluge	60 min
			Neovlaštena promjena podataka na domenama	20% od ukupnog broja registriranih .hr domena
		Registar naziva domena za .hr TLD	Nedostupnost usluge	180 min
			Neovlaštena promjena podataka na domenama	20% od ukupnog broja registriranih .hr domena
		Sustav za registriranje i administriranje sekundarne domene	Nedostupnost usluge	180 min
			Nedostupnost ovlaštenih registara	40% od ukupnog broja registara
		Usluga IXP	Nedostupnost usluge za 50% spojenih članica	8 sati
			Nedostupnost usluge za 75% spojenih članica	4 sata
			Nedostupnost usluge za sve spojene članice	2 sata
Poslovne usluge za središnja državna tijela		**Usluge u sustavu e-Građani**	Broj korisnika pogođenih prekidom	20%
			Trajanje incidenta	2 sata
		Poslovne usluge za korisnike državnog proračuna	Trajanje incidenta	1 sat
			Broj sektorskih korisnika pogođenih incidentom	jedan

Prilog 2. Obrazac inicijalne obavijesti o incidentu sa znatnim učinkom s uputama za popunjavanje

Inicijalna obavijest		
OSNOVNI PODACI		
Korisnik (organizacija)[1]	Puni naziv korisnika (organizacije)	
Kontakt osoba	Ime i prezime odgovorne osobe za izvješćivanje o incidentu	
Kontakt e-mail	Adresa e-pošte na koju se mogu po potrebi slati zahtjevi za dodatna objašnjenja	
Kontakt broj	Telefonski broj na koji se mogu po potrebi slati zahtjevi za dodatna objašnjenja	
Radi li se o incidentu informacijske sigurnosti?[2]	☐DA ☐NE	Informacija o tome je li incident nastao primarnim djelovanjem na IT razini (kibernetički napad, kvar opreme, pogrešna konfiguracija i slično – odgovor DA) ili se radi o vanjskim utjecajima (poplava, požar, krađa, elementarne nepogode i slično – odgovor NE)
Klasifikacija incidenta[3]	Choose an item.	Ako je moguće, klasificirajte incident u skladu s Nacionalnom taksonomijom računalno-sigurnosnih incidenta
Točno vrijeme otkrića incidenta	Datum i vrijeme kada je otkriven incident	
Postoje li saznanja o prekograničnom utjecaju? Ako postoje, opišite utjecaj.	Ako postoje, opišite rizike od manifestacije incidenta u ostalim zemljama EU. (Primjer: uslugu pružamo u Republici Sloveniji i gdje korisnici u ovom trenutku nemaju pristup usluzi)	
Postoje li saznanja o negativnom utjecaju na druge operatore ključnih usluga/sektore? Ako postoje, opišite utjecaj.	Ako postoje, opišite rizike od manifestacije incidenta u ostalim sektorima operatora ključnih usluga u RH. (Primjer: našu uslugu koriste korisnici iz sektora zdravstva i postoji mogućnost da raspoloživost njihovih usluga bude ugrožena)	
Kratki opis događaja i trenutačne situacije	Ukratko navedite najvažnije pojedinosti o incidentu, uključujući moguće uzroke, trenutačne učinke itd.	
Broj zahvaćenih korisnika	Ako nemate točan broj zahvaćenih korisnika unesite procjenu prema prosječnom broju korisnika u vrijeme otkrića incidenta	
Procjena ukupnog utjecaja incidenta	Odaberite	
Procjena dana dostave prijelaznog izvješća	Navedite procijenjeno vrijeme u kojem će biti dostavljeno prijelazno izvješće (prijelazno izvješće potrebno je dostaviti najkasnije tri dana[4] od podnošenja inicijalne obavijesti o incidentu)	

[1] Osnovni podaci o operatoru ključne usluge ili davatelju digitalnih usluga (predefinirani podaci)
[2] U slučaju da se radi o incidentima koji nisu primarno kibernetičke prirode (požar, poplava, krađa i slično)
[3] U skladu s Nacionalnom taksonomijom računalno-sigurnosnih incidenata (Prilog 5)
[4] U skladu s čl. 41. st. 1. Uredbe o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 68/2018.)

Prilog 3. Obrazac prijelaznog izvješća o incidentu sa znatnim učinkom s uputama za popunjavanje

Prijelazno izvješće		
OSNOVNI PODACI		
Opišite incident i kronologiju događaja, uključujući: • Kako je došlo do pojave incidenta (kronologija, vektor napada)? • Postoji li poveznica s nekim ranijim incidentom/događajem? • Kako je otkriven incident? • Jesu li treće strane uključene u razvoj/rješavanje incidenta? • Koji procesi kriznog upravljanja su započeti? • Je li najviša rukovodeća razina upoznata s razvojem događaja?	Navedite najvažnije pojedinosti o incidentu, uključujući moguće uzroke, trenutačne učinke itd.	
Trenutačni status incidenta	☐Dijagnostika ☐Oporavak	Navedite trenutni status incidenta
Klasifikacija incidenta [4]	Choose an item.	Ako je došlo do promjene u klasifikaciji incidenta, klasificirajte incident u skladu s Nacionalnom taksonomijom računalno-sigurnosnih incidenta
UČINAK INCIDENTA		
Incident je utjecao na	☐Povjerljivost podataka ☐Cjelovitost podataka ☐Dostupnost podataka, procesa i usluga	Navedite na koje od osnovne tri sastavnice informacijske sigurnosti (povjerljivost, cjelovitost, dostupnost) je incident imao utjecaj.
Incident je otkriven	Choose an item.	Navedite na koji je način došlo do spoznaje o postojanju incidenta
Koje usluge/procesi su zahvaćene incidentom (zaustavljene, ugrožene, usporene)?	Nabrojite sve usluge/procese u organizaciji koji su zahvaćeni pojavom incidenta. (Primjer: usluga internetskog bankarstva, proces nadzora prometne signalizacije…)	
Koliko dugo je zahvaćena usluga/proces bila pod negativnim učinkom	Za svaku od zahvaćenih usluga navedite razdoblje u kojem je ta usluga bila zaustavljena, ugrožena ili usporena. (Primjer: internetsko bankarstvo nedostupno tri sata, usporen rad 24 sata)	

incidenta (zaustavljena, ugrožena, usporena)?	
Koji IT sustavi su zahvaćeni incidentom, osobito: • Aplikacije, • Hardver, • Baze podataka, • Mrežna infrastruktura, • Ostalo.	Nabrojite IT sustave u organizaciji koji su zahvaćeni pojavom incidenta. (Primjer: aplikacija internetskog bankarstva, četiri poslužitelja u podatkovnom centru Rijeka, Oracle baza podataka V.X.Y, itd.)
Navedite broj krajnjih korisnika na koje je incident imao negativan učinak (u smislu izostanka ili narušavanja kvalitete usluge).	
RJEŠAVANJE INCIDENTA	
Koji su interni resursi angažirani na rješavanju incidenta?	(Primjer: pet djelatnika IT sektora, tri djelatnika pravne službe, Član Uprave, PR tim)
Koji su vanjski resursi angažirani na rješavanju incidenta (vanjski eksperti, dobavljači, pravne službe, PR)?	(Primjer: pet djelatnika tvrtke X zadužene za mrežu, jedan djelatnik tvrtke za krizno komuniciranje)
Navedite očekivani rok oporavka od incidenta?	(Primjer: prema prvim procjenama oporavak bi trebao završiti kroz dva do tri dana)
Koje su mjere/aktivnosti poduzete u svrhu oporavka od incidenta?	Navedite mjere/aktivnosti koje su poduzete u svrhu oporavka od incidenta. (Primjer: 1. Održani sastanci s Upravom, dobavljačima i nadležnim CSIRT-om; 2. Aktivirana rezervna lokacija; 3. PR tim održao konferenciju za medije upoznavši ih s detaljima incidenta; 4. Ostvaren kontakt s međunarodnim poslovnim partnerima u svrhu dolaska njihovih stručnjaka za tehnologiju koju koristimo…)
Jesu li aktivirani planovi očuvanja kontinuiteta poslovanja (BCP) i planovi oporavka u slučaju katastrofa (DRP)? Ako jesu, navedite osnovne aktivnosti iz tih planova koje su u tijeku.	(Primjer: aktivirana je rezervna lokacija na koju je preseljen dio zaposlenika kako bi usluga mogla nastaviti s funkcioniranjem; započet je oporavak podataka na primarnoj lokaciji korištenjem pričuvnih kopija…)

[4] Ako je došlo do promjene klasifikacije

Prilog 4. Obrazac završnog izvješća o incidentu sa znatnim učinkom s uputama za popunjavanje

Završno izvješće	
(prije popunjavanja Završnog izvješća potrebno je popuniti Prijelazno izvješće sa svim do tada poznatim informacijama.	
Vrijeme završetka incidenta	Datum i vrijeme kada je incident okončan
Ukupno trajanje incidenta	Navedite ukupno vrijeme trajanja incidenta
Ukupno vrijeme kroz koje je usluga bila potpuno ili djelomično nedostupna	Navedite ukupno vrijeme kroz koje je usluga bila potpuno ili djelomično nedostupna
Broj korisnika ključne usluge na koje je incident imao negativan učinak (u smislu izostanka ili narušavanja kvalitete usluge).	Ako je moguće, procijenite broj korisnika na koje je incident imao negativni učinak
Ukupan utjecaj incidenta	Odaberite
Je li postojao negativan utjecaj na druge operatore ključnih usluga/sektore? Ako je, opišite ga.	Opišite utjecaj incidenta na druge operatore ključnih usluga/sektore, ako je isti postojao. (Primjer: određeni operatori iz sektora bankarstva imali su prekid pružanja svoje usluge uslijed naše nemogućnosti da isporučimo električnu energiju)
Je li postojao prekogranični utjecaj? Ako je, opišite ga.	Opišite prekogranični utjecaj incidenta, ako je isti postojao. (Primjer: Naši korisnici u Italiji nisu mogli koristiti uslugu kroz period od četiri sata.)
Jesu li treće strane sudjelovale u rješavanju incidenta? Ako jesu, koje?	Navedite nazive i o aktivnosti trećih strana u rješavanju incidenta, ako su iste sudjelovale. (Primjer: Tvrtka A za krizno komuniciranje, Tvrtka B za nadzor mreže)
Jesu li u rješavanju incidenta sudjelovale službene institucije RH ili EU? Ako jesu, koje?	Navedite nazive i aktivnosti službenih institucija RH ili EU u rješavanju incidenta, ako su iste sudjelovale. (Primjer: Nacionalni CERT, MUP, ENISA ...)
ANALIZA UZROKA	
Ako je provedena raščlamba primarnog uzroka, navedite osnovne zaključke.	Priložite analizu uzroka i posljedica incidenta (raščlamba primarnog uzroka).
Je li planirano uvođenje novih ili nadogradnja postojećih sigurnosnih mjera koje mogu spriječiti buduću pojavu incidenta ove vrste? Ako je, navedite i opišite kojih.	Opišite aktivnosti koje se planiraju provesti kako bi se spriječila buduća pojava incidenta ove vrste

Prilog 5. Nacionalna taksonomija računalno-sigurnosnih incidenata - Operativni učinak napada (0)

Oznaka	Vrijednost	Oznaka	Potkategorije	Opis
(01)	Uspješno ostvarena kompromitacija	(011)	*Web Defacement*	*Web Defacement* podrazumijeva kompromitirano *web* sjedište s izmijenjenim izgledom i sadržajem *web* stranice.
		(012)	Sustav zaražen zlonamjernim kodom	Podrazumijeva računalo (npr. PC, pametni telefon, IoT i sl.) zaraženo zlonamjernim kodom.
		(013)	*C&C*	*C&C* podrazumijeva upravljački poslužitelj za nadzor i upravljanje računalima koja su dio botneta. Također može služiti kao točka prikupljanja ukradenih podataka s različitih botova.
		(014)	Korisnički račun	Korisnički račun podrazumijeva kompromitaciju korisničkog računa za pristup nekom web servisu ili računalnom sustavu.
(02)	Zlonamjerno web sjedište	(021)	Malware URL	Poveznica do postavljenog zlonamjernog programskog koda na kompromitiranom web sjedištu ili na zlonamjernom web sjedištu registriranom u tu svrhu.
		(022)	Phishing URL	Poveznica do lažne Internet stranice na kompromitiranom web sjedištu ili sjedištu registriranom u svrhu krađe povjerljivih podataka.
		(023)	*Spam URL*	Poveznica do kompromitiranog web sjedišta ili web sjedišta registriranog s ciljem postavljanja neovlaštenog reklamnog sadržaja.
(03)	Pokušaj neovlaštenog pristupa	(031)	Pogađanje zaporki	Pogađanje zaporki podrazumijeva neovlašten pokušaj pristupa računalnom sustavu višestrukim pogađanjem zaporke.
		(032)	Pokušaj iskorištavanja ranjivosti	Pokušaj iskorištavanja ranjivosti podrazumijeva pokušaj iskorištavanja ranjivosti na računalnom sustavu kako bi se ostvario neovlašten pristup ili utjecalo na tajnost ili cjelovitost podataka.

(04)	Prikupljanje informacija	(041)	Skeniranje	Skeniranje podrazumijeva neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima.
		(042)	*Sniffing*	*Sniffing* podrazumijeva neovlašteno presretanje mrežnog prometa.
(05)	Dostupnost	(051)	DoS - Volumetrički napad	Volumetrički napad podrazumijeva napad slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti.
		(052)	DoS - Napad na aplikacijskom sloju	Napad na aplikacijskom sloju podrazumijeva slanje zahtjeva prema računalnom sustavu s ciljem iskorištavanja resursa sustava ili iskorištavanje sigurnosnog propusta koje dovodi do prestanka rada aplikacije.
		(053)	Ispad usluge (eng. *Outage*)	Podrazumijeva neočekivani gubitak dostupnosti izazvan greškom u radu sustava, ljudskom greškom ili namjernim lokalnim sabotiranjem sustava. ***Ovaj tip incidenta odnosi se isključivo na tijela definirana Zakonom o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga (NN 64/2018).***
(06)	Zlonamjerno rudarenje kriptovalute (eng. *Cryptojacking*)			Neovlašteno iskorištavanje računalnih resursa za rudarenje kriptovalute. Najčešći oblici vektora *cryptojacking* napada dolaze putem *phishing* poruka ili prilikom posjete web sjedištu koje ima ugrađenu *cryptomining* skriptu.
(07)	Neželjene elektroničke poruke, uvredljiv	(071)	*Spam*	*Spam* podrazumijeva neželjenu elektroničku poruku reklamnog sadržaja.

	sadržaj, uznemiravanje, dezinformiranje	(072)	*Hoax*	*Hoax* podrazumijeva poruku elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja.
		(073)	*Zavaravanje korisnika*	Navođenje korisnika na dijeljenje lažnog sadržaja, najčešće putem IM aplikacija, s ciljem prikupljanja marketinških podataka ili poticanje korisnika na razne pretplate.
(08)	Ciljani napad – *APT* (*eng. Advanced persistent threat*)			*APT* podrazumijeva ciljani napad na određenu žrtvu uz korištenje većeg broja naprednih tehnika i tehnologija.
(09)	Prijevare	(091)	*Phishing*	• Pokušaj navođenja korisnika na odavanje povjerljivih podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte). • Pokušaj navođenja korisnika na pokretanje zlonamjernog programa putem raznih komunikacijskih kanala (najčešće elektroničke pošte). • Napad u kojima napadač lažnim predstavljanjem pokušava steći financijsku korist od ciljane žrtve. • Podrazumijeva širok spektar napada kojim se pokušava manipulirati žrtvom, primjerice *smishing*, *vishing*, *catphishing*, *whaling* i druge.
		(092)	*Spear Phishing*	Vrsta *phishing* incidenta kod kojeg napadač cilja točno određenu žrtvu o kojoj unaprijed istraži informacije kako bi ih mogao iskoristiti u svoju korist.
		(093)	*Scam*	Pokušaji vještog navođenja potencijalne žrtve na djelovanje u korist prevaranta (najčešće putem elektroničke pošte). Najpoznatiji oblik je „*nigerian scam*“ ili „*419 fraud*“.

		(094)	*Iznuda*	Pokušaj navođenja korisnika na plaćanje iznude, najčešće lažnim informacijama i zastrašivanjem.
		(095)	*Poslovna prijevara*	Napadi kod kojih napadač lažnim predstavljanjem pokušava steći ili stekne financijsku korist od ciljanog poslovnog korisnika. Jedan on najčešćih oblika ovakvih napada su tzv. „CEO *fraud*" ili „BEC" (*Business Email Compromise*).
(010)	Ostalo			Podrazumijeva neželjene događaje koji ne mogu biti opisani ranije navedenim atributima, a koji bi se mogli okarakterizirati kao računalno-sigurnosni incident.