



CARNET
znanje povezuje

CERT.hr
surfaj sigurnije



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)

Sadržaj

Status	1
Područje primjene i izuzeci.....	1
Protokol dostave obavijesti o incidentima sa znatnim učinkom	2
Inicijalna obavijest.....	2
Prijelazna izvješća.....	2
Završno izvješće.....	3
Komunikacija tijekom trajanja incidenta.....	3
Prilog 1. Kriteriji za prepoznavanje znatnog učinka	4
Prilog 2. Obrazac inicijalne obavijesti o incidentu sa znatnim učinkom s uputama za popunjavanje.....	10
Prilog 3. Obrazac prijelaznog izvješća o incidentu sa znatnim učinkom s uputama za popunjavanje.....	11
Prilog 4. Obrazac završnog izvješća o incidentu sa znatnim učinkom s uputama za popunjavanje.....	13
Prilog 5. Nacionalna taksonomija računalno-sigurnosnih incidenata - Operativni učinak napada (O).....	14

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. Ove Smjernice primjenjuju se od 2. 11. 2018.

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 na sljedeći način:
 - Nacionalni CERT
 - Informacije o incidentu prijavljuju se na telefonski broj **01 6661 650** prema uputama opisanim na **www.cert.hr/zks-incident**
 - Inicijalne obavijesti, prijelazna i završna izvješća na e-mail adresu zks-incident@cert.hr
 - 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 na e-mail adresu cert@zsis.hr

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.

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.
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 (*on-line* obrazac, dostava skeniranog obrasca i slično) bit će predočen nakon identifikacije operatora ključnih usluga i davatelja digitalnih usluga.
5. 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.
2. Protokol dostave završnog izvješća (*on-line* obrazac, dostava skeniranog obrasca i slično) bit će predloženi 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 uspostaviti će neposredne kanale komunikacije (telefon, e-mail) za razmjenu svih operativnih informacija i podataka (npr. uzorci zlonamjernih programa, uzorak mrežnog prometa) neovisno o ovim Smjernicama definiranim izvješćima.

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 prijena	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 kapaciteta 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-	Ugrožavanje integriteta prometno-upravljačkog, signalno-sigurnosnog ili	Bez iznimke	

		upravljačkim i signalno-sigurnosnim podsustavom	elektro-energetskog podsustava	
		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 VTMS i pružanja VTS usluga	Onemogućeno korištenje punih funkcionalnosti sustava za nadzor i upravljanje pomorskim prometom VTMS 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 tri 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 tri 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 tri 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	
	Ukrcaj i iskrcaj tereta u lukama u međunarodnom i domaćem prometu	Nedostupnost i ograničenost operativnog sustava	Nemogućnost obavljanja ključnih operacija u periodu duljem od tri dana	
		Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od tri dana može	

	Vodni prijevoz			uzrokovati zastoje u ovisnim sektorima
			Važnost održavanja dostatne razine usluge	Ako incident uzrokuje nemogućnost obavljanja ključne usluge u vremenu duljem od tri 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 tri 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	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. Direktive (EU) 2015/2366 o platnim uslugama na unutarnjem tržištu (PSD2 Direktiva)	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	pet minuta
		Usluge središnjih drugih ugovornih strana (CCP)	Trajanje incidenta	pet minuta
Zdravstveni sektor	Primarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	osam sati	
		Nedostupnost Zdravstvene VPN mreže HealthNet	osam sati	
		Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati	
		Nedostupnost informacijskog sustava hitne medicinske pomoći	osam sati	
	Sekundarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	osam sati	
		Nedostupnost Zdravstvene VPN mreže HealthNet	osam sati	
		Nedostupnost odobrenog programskog rješenja za pružatelja zdravstvene zaštite	12 sati	
		Nedostupnost bolničkog informacijskog sustava u općoj bolnici	jedan sat	
	Tercijarna zdravstvena zaštita	Nedostupnost Centralnog zdravstvenog informacijskog sustava Hrvatske	osam sati	
		Nedostupnost Zdravstvene VPN mreže HealthNet	osam sati	
		Nedostupnost bolničkog informacijskog sustava u kliničkom bolničkom centru	jedan sat	
		Nedostupnost bolničkog informacijskog sustava u kliničkoj bolnici	jedan sat	
		Nedostupnost bolničkog informacijskog sustava u klinici	jedan sat	
	Transfuzijska medicina i transplantacija organa	Nedostupnost informacijskog sustava za djelatnost transfuzijske medicine	osam sati	
		Nedostupnost Zdravstvene VPN mreže HealthNet	osam sati	

			Nedostupnost koordinatora Nacionalnog transplantacijskog programa	jedan 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	osam 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	osam sati
			Nedostupnost Zdravstvene VPN mreže HealthNet	osam sati
Opskrba vodom za piće i njezina distribucija		Opskrba krajnjih korisnika	Prekid opskrbe	Broj priključaka kućanstava * broj dana prekida>1000
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	osam sati		
	Nedostupnost usluge za 75% spojenih članica	četiri sata		

			Nedostupnost usluge za sve spojene članice	dva sata
Poslovne usluge za središnja državna tijela		Usluge u sustavu e-Građani	Broj korisnika pogođenih prekidom	20%
			Trajanje incidenta	dva sata
		Poslovne usluge za korisnike državnog proračuna	Trajanje incidenta	jedan 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	<input type="checkbox"/> DA <input type="checkbox"/> 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.
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 (predefimirani 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: <ul style="list-style-type: none"> • 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	<input type="checkbox"/> Dijagnostika <input type="checkbox"/> 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	<input type="checkbox"/> Povjerljivost podataka <input type="checkbox"/> Cjelovitost podataka <input type="checkbox"/> 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 incidenta (zaustavljena, ugrožena, usporena)?	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)	

<p>Koji IT sustavi su zahvaćeni incidentom, osobito:</p> <ul style="list-style-type: none"> • Aplikacije, • Hardver, • Baze podataka, • Mrežna infrastruktura, • Ostalo. 	<p>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.)</p>
<p>Navedite broj krajnjih korisnika na koje je incident imao negativan učinak (u smislu izostanka ili narušavanja kvalitete usluge).</p>	
RJEŠAVANJE INCIDENTA	
<p>Koji su interni resursi angažirani na rješavanju incidenta?</p>	<p>(Primjer: pet djelatnika IT sektora, tri djelatnika pravne službe, Član Uprave, PR tim)</p>
<p>Koji su vanjski resursi angažirani na rješavanju incidenta (vanjski eksperti, dobavljači, pravne službe, PR)?</p>	<p>(Primjer: pet djelatnika tvrtke X zadužene za mrežu, jedan djelatnik tvrtke za krizno komuniciranje)</p>
<p>Navedite očekivani rok oporavka od incidenta?</p>	<p>(Primjer: prema prvim procjenama oporavak bi trebao završiti kroz dva do tri dana)</p>
<p>Koje su mjere/aktivnosti poduzete u svrhu oporavka od incidenta?</p>	<p>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...)</p>
<p>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.</p>	<p>(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...)</p>

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
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 (O)

Oznaka	Vrijednost	Oznaka	Potkategorije	Opis
(01)	Kompromitacija	(011)	<i>Malware URL</i>	Malware URL podrazumijeva kompromitiran web poslužitelj s postavljenim zlonamjernim kodom.
		(012)	<i>Phishing URL</i>	Phishing URL podrazumijeva kompromitiran web poslužitelj s postavljenom lažiranom stranicom čija je svrha krađa podataka.
		(013)	<i>Spam URL</i>	Spam URL podrazumijeva kompromitiran web poslužitelj s neovlašteno postavljenim reklamnim sadržajem.
		(014)	<i>Web Defacement</i>	Web Defacement podrazumijeva kompromitiran web poslužitelj s izmijenjenim izgledom i sadržajem web stranice.
		(015)	<i>Sustav zaražen zlonamjernim kodom</i>	Podrazumijeva računalo ili neki drugi uređaj zaražen zlonamjernim kodom. Botovi, tj. računala pod kontrolom napadača spadaju u ovu kategoriju.
		(016)	<i>C&C</i>	C&C podrazumijeva kontrolni poslužitelj za nadzor i upravljanje računalima koja su dio botneta.
		(017)	<i>Korisnički račun</i>	Korisnički račun podrazumijeva kompromitaciju korisničkog računa.
(02)	Prikupljanje informacija	(021)	Skeniranje	Skeniranje podrazumijeva neovlašteno automatizirano prikupljanje informacija o računalnim mrežama i sustavima.
		(022)	<i>Phishing</i>	Navođenje korisnika na odavanje podataka putem raznih komunikacijskih kanala (najčešće elektroničke pošte).
		(023)	<i>Sniffing</i>	Sniffing podrazumijeva neovlašteno presretanje mrežnog prometa.
(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)	Uskraćivanje dostupnosti	(041)	Volumetrički napad	Volumetrički napad podrazumijeva napad slanjem velikog broja IP paketa s ciljem zagušenja mrežne propusnosti.
		(042)	Napad na aplikacijskom sloju	Napad na aplikacijskom sloju podrazumijeva slanje većeg broja zahtjeva prema računalnom sustavu s ciljem iskorištavanja resursa sustava ili iskorištavanje sigurnosnog propusta koje dovodi do prestanka rada aplikacije.
(05)	Neželjene elektroničke poruke, uvredljiv sadržaj, uznemiravanje, dezinformiranje	(051)	<i>Spam</i>	Spam podrazumijeva neželjenu elektroničku poruku reklamnog sadržaja.
		(052)	<i>Hoax</i>	Hoax podrazumijeva poruku elektroničke pošte neistinitog sadržaja, poslana s ciljem zastrašivanja ili dezinformiranja primatelja.
(06)	Ciljani napad – APT (eng. Advanced persistent threat)			APT podrazumijeva ciljani napad na određenu žrtvu uz korištenje većeg broja naprednih tehnika i tehnologija
(07)	Prijevare			Ova klasa događaja uključuje događaje koji se mogu kategorizirati kao kibernetički kriminal, a podrazumijeva razne vrste prijevara na internetu, od lažnog predstavljanja, prijevara prilikom trgovine na internetu i sl. U ovu klasu događaja ne spadaju financijske prijevare koje uključuju instalaciju zlonamjernoga koda.
(08)	Ostalo			Podrazumijeva sve događaje koji ne mogu biti opisani ranije navedenim atributima, a za koje korisnik smatra da se radi o računalno-sigurnosnom incidentu.