Opće smjernice za provedbu obveze obavještavanja o značajnim incidentima

Sadržaj

Uvod

Na temelju članka 72. stavka 2. Uredbe o kibernetičkoj sigurnosti („Narodne novine“, br. 135/24., u daljnjem tekstu: UKS) Nacionalni centar za kibernetičku sigurnost i Nacionalni CERT, kao nadležni CSIRT-ovi donose Opće smjernice za provedbu obveze obavještavanja o značajnim incidentima (u daljnjem tekstu: Opće smjernice) uz suglasnost središnjeg državnog tijela za kibernetičku sigurnost.

Nadležni CSIRT-ovi su prilikom donošenja Općih smjernica vodili računa o ENISA-inim tehničkim smjernicama o parametrima za informacije u svrhu obavještavanja ENISA-e temeljem članka 42. stavka 2. Zakona o kibernetičkoj sigurnosti („Narodne novine“, br. 14/24., u daljnjem tekstu: ZKS) u kojem se navodi obveza obavještavanja jedinstvene kontaktne točke (čije poslove po članku 61. ZKS-a obavlja Nacionalni centar za kibernetičku sigurnost) o značajnim incidentima, ostalim incidentima, kibernetičkim prijetnjama i izbjegnutim incidentima o kojima su ih ključni i važni subjekti obavijestili na temelju članaka 37. i 39. ZKS-a.

Opće smjernice sadrže upute i pojašnjenja procesa obavještavanja o značajnim incidentima, pojašnjenja u vezi primjene kriterija za utvrđivanje značajnih incidenata, načine obavještavanja nadležnog CSIRT-a o značajnom incidentu, vrste obavijesti i rokove za dostavu, postupanje u slučaju pojave značajnog incidenta koji obuhvaća više sektora, podsektora ili vrsta subjekata te obrasce za obavještavanje uz upute za njihovo ispunjavanje.

Obrasci koji se nalaze u Prilogu Općih smjernica integrirani su u obliku web obrazaca u Nacionalnu platformu za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima (dalje u tekstu: Platforma PiXi) prema članku 43. ZKS-a, Poglavlju IV. UKS-a i članku 15. Zakona o provedbi Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor („Narodne Novine“, br. 136/24.). Pristup Platformi PiXi imaju isključivo ovlaštene osobe putem Nacionalnog identifikacijskog i autentifikacijskog sustava (dalje u tekstu: NIAS).

Kriteriji za utvrđivanje značajnih incidenata

Značajan incident je svaki incident koji ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata iz članaka 59. do 62. UKS-a, uzimajući u obzir kriterijske pragove, kada su propisani.

U slučaju da je ispunjen kriterij iz članka 62. UKS-a, odnosno u slučaju da su se dogodila dva ili više incidenta s istim temeljnim uzrokom u razdoblju od šest mjeseci koji zajedno ispunjavaju najmanje jedan kriterij za značajan incident iz članaka 59. do 61. UKS-a, onda se za potrebe obavještavanja svi ti incidenti zajednički smatraju jednim značajnim incidentom. U tom slučaju subjekt treba poslati jednu obavijest koja obuhvaća sve navedene incidente. U obavijesti kroz opis incidenta mora biti navedeno da se radi o obavijesti koja obuhvaća više incidenata koji su po članku 62. UKS-a zajednički ispunili najmanje jedan kriterij za značajan incident iz članaka 59. do 61. UKS-a.

Za subjekte iz članka 22. ZKS-a koji se vode i u Posebnom registru subjekata, odnosno za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja, primjenjuju se posebna pravila za utvrđivanje slučajeva u kojima se incident smatra značajnim prema Provedbenoj uredbi Komisije (EU) 2024/2690 od 17. listopada 2024. o utvrđivanju pravila za primjenu Direktive (EU) 2022/2555.

Načini obavještavanja nadležnog CSIRT-a

Obavještavanje o značajnim incidentima provodi se ispunjavanjem web obrazaca dostupnih u okviru Platforme PiXi na poveznici https://pixi.carnet.hr/.

U slučaju nedostupnosti Platforme PiXi zbog tehničkih poteškoća, najavljenog redovnog održavanja, izvanrednog ispada servisa ili nedostupnosti NIAS-a što uzrokuje nemogućnost pristupa Platformi PiXi, subjekt o značajnom incidentu obavještava nadležni CSIRT ispunjavanjem obrazaca koji su dostupni na sljedećim poveznicama (isti obrasci su dostupni na obje poveznice):

- https://www.ncsc.hr/hr/obrasci-za-prijavu-znacajnih-incidenata
- https://www.cert.hr/zks-incident

Ispunjeni obrasci dostavljaju se putem e-pošte nadležnom CSIRT-u (sukladno nadležnostima iz Priloga III. ZKS-a) na sljedeće adrese:

- Nacionalni centar za kibernetičku sigurnost – incident@ncsc.hr
- Nacionalni CERT – zks-incident@cert.hr

U slučaju dostave obrazaca putem e-pošte, subjekti trebaju naknadno unijeti informacije o značajnim incidentima na Platformu PiXi čim ona ponovno postane dostupna.

Vrste obavijesti i rokovi za dostavu

Kategorizirani subjekti dužni su nadležnom CSIRT-u dostavljati sljedeće vrste obavijesti o značajnom incidentu unutar sljedećih rokova (čl. 65. do 71. UKS-a):

- **rano upozorenje o značajnom incidentu** – bez odgode, a najkasnije u roku od 24 sata od trenutka saznanja za značajan incident;
- **početnu obavijest o značajnom incidentu** – bez odgode, a najkasnije u roku od 72 sata od trenutka saznanja za značajan incident;
- **privremeno izvješće o značajnom incidentu** – na zahtjev nadležnog CSIRT-a u zadanom roku (od 48 sati do 7 dana);
- **završno izvješće o značajnom incidentu** – najkasnije u roku od 30 dana od dana dostave početne obavijesti o značajnom incidentu;
- **izvješće o napretku** – u slučaju da nije moguće dostaviti završno izvješće unutar roka jer incident još traje, dostavlja se izvješće o napretku umjesto završnog izvješća; unutar svakih sljedećih 30 dana trajanja incidenta dostavlja se novo izvješće o napretku, odnosno završno izvješće ako je incident završen.

Iznimno, prema čl. 68. UKS-a, pružatelji usluga povjerenja nisu dužni nadležnom CSIRT-u dostaviti rano upozorenje, već su dužni, bez odgode, a najkasnije u roku od **24 sata** od trenutka saznanja za značajan incident dostaviti **početnu obavijest o značajnom incidentu**. Preostale obavijesti dužni su dostaviti u istim rokovima kao i drugi subjekti.

Značajan incident koji obuhvaća više sektora, podsektora ili vrsta subjekata

Ako je subjekt kategoriziran samo u **jedan** sektor, podsektor ili vrstu subjekta (u daljnjem tekstu: sektor), onda o značajnom incidentu uvijek obavještava samo CSIRT koji je nadležan za taj sektor (sukladno Prilogu III. ZKS-a).

U slučaju da je subjekt kategoriziran u **više** sektora, te se dogodi značajan incident koji obuhvaća poslovanje subjekta u više sektora, **subjekt može poslati jednu obavijest za sve obuhvaćene sektore, ako je za te sektore nadležan isti CSIRT**. Ako značajan incident obuhvaća poslovanje subjekta u više sektora za koje **nije nadležan isti CSIRT**, onda subjekt treba slati **zasebne obavijesti svakom CSIRT-u** za sektore iz njihove nadležnosti.

Kod slanja obavijesti putem Platforme PiXi, subjekt može uvijek, neovisno o nadležnostima, ispuniti samo jedno rano upozorenje o značajnom incidentu u kojem navodi sve obuhvaćene sektore. Platforma PiXi će automatski, po potrebi, nakon spremanja ranog upozorenja razdvojiti to rano upozorenje na više ranih upozorenja za svaki nadležni CSIRT. U sljedećim koracima (početna obavijest i ostale vrste obavijesti) subjekt zasebno obavještava svaki nadležni CSIRT sukladno sektorima za koje je taj CSIRT nadležan.

Primjerice, pretpostavimo da je jedan subjekt kategoriziran u sektorima energetike, prometa i istraživanja. Za sektore energetike i prometa nadležni CSIRT je Nacionalni centar za kibernetičku sigurnost, dok je za sektor istraživanja nadležni CSIRT Nacionalni CERT.

Ako je značajan incident obuhvatio poslovanje subjekta u sektorima energetike i prometa, ali ne i u sektoru istraživanja, onda subjekt može poslati samo jedno rano upozorenje, početnu obavijest i završno izvješće, jer je nadležan CSIRT i za sektor energetike i za sektor prometa Nacionalni centar za kibernetičku sigurnost.

Ako je značajan incident obuhvatio poslovanje subjekta u sva tri sektora u kojima je subjekt kategoriziran (energetika, promet i istraživanje), tada subjekt mora slati zasebne obavijesti sukladno nadležnostima. Zasebno rano upozorenje, početnu obavijest i završno izvješće za sektor energetike i prometa treba poslati Nacionalnom centru za kibernetičku sigurnost, te zasebno rano upozorenje, početnu obavijest i završno izvješće za sektor istraživanja treba poslati Nacionalnom CERT-u. Ako subjekt šalje obavijest putem Platforme PiXi, može ispuniti samo jedno rano upozorenje te označiti sektore prometa, energetike i istraživanja, te će Platforma PiXi automatski nakon spremanja stvoriti dva rana upozorenja – jedno za sektor energetike i prometa za Nacionalni centar za kibernetičku sigurnost i drugo za sektor istraživanja za Nacionalni CERT. Nakon toga, u sljedećim koracima subjekt zasebno ispunjava dvije početne obavijesti i ostale vrste obavijesti za svaki od dva nadležna CSIRT-a.

Upute za ispunjavanje obrazaca

Obrasci na Platformi PiXi i obrasci na prethodno navedenim poveznicama su ekvivalentni te se ove upute za ispunjavanje obrazaca odnose na oba načina obavještavanja o značajnom incidentu. U nastavku su navedena polja obrazaca za svaku vrstu obavijesti te upute kako ih ispuniti.

Pojedina polja (poput naziva subjekta i OIB-a subjekta) se na Platformi PiXi popunjavaju automatski.

Polja označena sa zvjezdicom (*) su obavezna u tom obrascu.

Rano upozorenje o značajnom incidentu

Naziv subjekta*

Puni naziv subjekta.

OIB subjekta*

Osobni identifikacijski broj (OIB) subjekta.

Kontakt podaci prijavitelja*

Ime, prezime, broj telefona/mobitela i adresa e-pošte prijavitelja, odnosno kontakt osobe.

Sektor, podsektor i vrsta subjekta*

Potrebno je odabrati (na Platformi PiXi), odnosno navesti (kod ručnog popunjavanja obrasca) svaki sektor, podsektor ili vrstu subjekta po kojima je subjekt kategoriziran, a koji su zahvaćeni incidentom. Popis sektora, podsektora i vrsti subjekata dostupan je u Prilogu I. UKS-a. Dozvoljeno je odabrati odnosno navesti više sektora, podsektora i vrsta subjekata sukladno uputama u poglavlju „Značajan incident koji obuhvaća više sektora, podsektora ili vrsta subjekata" Općih smjernica.

Po kojim kriterijima je incident značajan

Potrebno je odabrati, odnosno navesti kriterije za utvrđivanje značajnih incidenata koje ovaj incident ispunjava, sukladno poglavlju „Kriteriji za utvrđivanje značajnih incidenata" Općih smjernica.

U ranom upozorenju ovo polje nije obavezno kako bi se subjektu olakšalo obavještavanje u ranoj fazi odgovora na incident – primjerice, ako se dogodi ucjenjivački (eng. *ransomware*) napad zbog kojega je onemogućen cijeli informacijski sustav subjekta, subjektu može biti očito da se radi o značajnom incidentu bez da točno provjerava i navodi koji su sve kriteriji ispunjeni.

Kategorija i potkategorija incidenta*

Potrebno je odabrati odnosno navesti procjenu kojoj kategoriji i potkategoriji pripada incident prema tablici „Operativni učinak napada" iz Nacionalne taksonomije kibernetičkih incidenata koja je dostupna na sljedećim poveznicama (ista taksonomija je dostupna na obje poveznice):

- https://www.ncsc.hr/hr/nacionalna-taksonomija-incidenata

- https://www.cert.hr/nacionalna-taksonomija-incidenata

Na Platformi PiXi dovoljno je odabrati samo potkategoriju incidenta te će se kategorija automatski ispuniti. Kod popunjavanja obrasca za slanje putem e-pošte, poželjno je, uz kategoriju i potkategoriju, navesti njihovu brojčanu oznaku, npr. kategorija „Uspješno ostvarena kompromitacija", potkategorija „Ucjenjivački napad" (oznaka O41).

Datum i vrijeme kada je otkriveno da se radi o značajnom incidentu*

Datum i vrijeme (po lokalnoj vremenskoj zoni u Hrvatskoj, CET odnosno CEST) kada je subjekt otkrio da se radi o značajnom incidentu.

Datum i vrijeme kada je incident otkriven*

Datum i vrijeme (po lokalnoj vremenskoj zoni u Hrvatskoj, CET odnosno CEST) kada je subjekt otkrio incident. Nije nužno isto kao i prošlo polje, jer je moguće da je subjekt u jednom trenutku otkrio incident, a da je tek naknadno otkrio da je taj incident značajan, tj. da ispunjava najmanje jedan kriterij za utvrđivanje značajnih incidenata.

Datum i vrijeme kada je incident nastao

Datum i vrijeme (po lokalnoj vremenskoj zoni u Hrvatskoj, CET odnosno CEST) kada je incident nastao odnosno trenutna procjena (ako istraga još nije gotova) pojave najranije poznate aktivnosti povezane s ovim incidentom (npr. vrijeme neovlaštene prijave napadača na sustav subjekta ili vrijeme kada je računalo na mreži subjekta zaraženo). Polje nije obavezno jer je moguće da istragom još nije utvrđeno kada je incident nastao.

Sažetak incidenta*

Sažeti opis incidenta, odnosno ključne informacije poput:

- Što se ukratko dogodilo (na temelju trenutno poznatih informacija)?
- Koji je utjecaj incidenta (ima li utjecaja na poslovanje/pružanje usluge, jesu li ukradeni osjetljivi podaci)?
- Koje je trenutno stanje oporavka od incidenta?

Opis osnovnih značajki incidenta*

U opisu treba navesti trenutno dostupne informacije o incidentu. S obzirom na to da se radi tek o ranom upozorenju, ne očekuje se da subjekt ima odgovor na sva pitanja navedena u nastavku, već samo da navede ključne informacije koje su trenutno dostupne.

Kako bi se olakšalo strukturirano popunjavanje ovog polja i ekvivalentnih polja u ostalim vrstama obavijesti, subjekt kod popunjavanja može pratiti sljedeća pitanja:

- Opće informacije o incidentu:
  - Što se dogodilo?
  - Kada i kako je incident otkriven?
  - Tko je sve obaviješten o incidentu (npr. pojedine državne institucije, korisnici, poslovni partneri, javnost)?

- Osim djelatnika subjekta, je li još netko uključen u odgovor na incident (npr. vanjske tvrtke koje pružaju usluge održavanja infrastrukture ili vanjske tvrtke specijalizirane za odgovor na incidente)?
- Je li ovo prvi put da se ovakav incident dogodio ili subjekt ima prethodnih iskustva sa sličnim incidentima? Potrebno je navesti i ako se radi o incidentu koji je značajan po članku 62. UKS-a (značajan incident koji obuhvaća dva ili više incidenta s istim temeljnim uzrokom u razdoblju od šest mjeseci koji zajedno ispunjavaju najmanje jedan kriterij za značajan incident iz članaka 59. do 61. UKS-a). U tom slučaju treba ukratko opisati i pojedine incidente i njihov zajednički utjecaj.

- Utjecaj incidenta:
  - Koji je utjecaj incidenta na poslovanje/pružanje usluge?
  - Koliko dugo je trajao utjecaj incidenta na poslovanje te traje li još uvijek?
  - Ako je bilo utjecaja na pružanje usluge, koliko je korisnika/primatelja usluge zahvaćeno?
  - Je li bilo javnih objava vezanih uz ovaj incident, npr. članaka u medijima ili objava na mrežnim stranicama napadača (npr. prijetnja objave ukradenih podataka)?
  - Ako se radi o napadu, je li ostvarena ikakva komunikacija s napadačem (npr. je li se napadač javljao putem e-pošte ili telefona i tražio otkupninu, je li subjekt ili netko drugi stupao u kontakt s napadačem i sl.)?
  - Koji je tehnički utjecaj incidenta na infrastrukturu?
  - Je li narušen integritet ili dostupnost nekog dijela infrastrukture, npr. zbog zaključavanja/šifriranja podataka ili DDoS napada? Ako je, jesu li obuhvaćene i pričuvne kopije (eng. *backups*) odnosno drugi redundantni dijelovi infrastrukture?
  - Je li narušena povjerljivost podataka, odnosno jesu li ukradeni neki podaci?
- Oporavak i podizanje razine sigurnosti/ublažavanje rizika:
  - Koji je plan za oporavak od incidenta i za implementaciju dodatnih sigurnosnih mjera odnosno mjera ublažavanja rizika (za povratak infrastrukture u prijašnje stanje te za podizanje razine sigurnosti odnosno ublažavanja rizika)? Koje je trenutno stanje oporavka i implementacije sigurnosnih mjera?
  - Postoje li planovi za odgovor na incident, kontinuitet poslovanja i oporavak od nesreće te jesu li aktivirani?
- Istraga:
  - Koja je kronologija incidenta, odnosno relevantnih događaja (kada je incident započeo, kada je incident otkriven, kada je otkriveno da se radi o značajnom incidentu, koje su do sada otkrivene aktivnosti napadača ako se radi o napadu, odnosno koje su druge otkrivene relevantne aktivnosti)?
  - Što se zna o uzroku incidenta? Radi li se o kibernetičkom napadu ili o incidentu uzrokovanom nenamjernom greškom?
  - Ako se radi o napadu – koji je inicijalni vektor napada, koju je infrastrukturu napadač koristio za napad te koje su druge taktike, tehnike i procedure korištene u napadu? Jesu li dostupne ikakve informacije o napadaču (o pojedincu ili skupini koja stoji iza napada)?

Indikatori kompromitacije

Indikatori kompromitacije povezani s ovim incidentom, ako su dostupni: IP adrese, domene, URL-ovi, adrese e-pošte, kriptografski sažeci (eng. *hash*) i sl. Indikatore je moguće navesti izravno u obrascu i/ili dostaviti u prilogu na Platformi PiXi odnosno u privitku poruke e-pošte. Poželjno je da se za svaki indikator navede i kontekst indikatora (npr. je li s otkriven zlonamjerni dolazni promet s određene IP adrese prema mreži subjekta ili odlazni promet iz mreže subjekta prema toj adresi).

Poželjno je da se indikatori kompromitacije navedu u obliku koji nije moguće slučajno otvoriti (eng. *defanged*), npr. 198.51.100[.]5 umjesto 198.51.100.5, example[.]com umjesto example.com, hxxps://example[.]com/file.html umjesto https://example.com/file.html, username@example[.]com umjesto username@example.com i sl.

Za slučaj da se dio indikatora ili svi indikatori dostavljaju kroz datoteke u privitku, potrebno je navesti nazive dostavljenih datoteka uz kratki opis što je u njima.

Prilozi

Bilo kakve druge dodatne informacije moguće je dostaviti u prilogu na Platformi PiXi odnosno u privitku poruke e-pošte. Ako se privitak šalje kroz e-poštu, ovdje je potrebno navesti nazive dostavljenih datoteka uz kratki opis što je u njima.

Postoji li sumnja na napad putem opskrbnog lanca*

Postoji li sumnja da je uzrok incidenta kompromitacija treće strane koja se proširila na subjekt koji prijavljuje incident (napad putem opskrbnog lanca na subjekt)? Ako da, potrebno je navesti dodatne informacije (o kojoj se trećoj strani radi, je li se treća strana javila subjektu ili je subjekt sam saznao za kompromitaciju).

Postoji li sumnja da posljedica ovog incidenta može biti kompromitacija trećih strana, npr. klijenata ili poslovnih partnera od subjekta koji prijavljuje incident (napad putem opskrbnog lanca iz subjekta prema drugima)? Ako da, potrebno je navesti dodatne informacije te je li subjekt ili netko drugi javio potencijalnim žrtvama napada da su ugroženi.

Postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem*

Postoji li sumnja da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem, tj. da se radi o kibernetičkom napadu iza kojega stoji pojedinac ili grupa, ili se sumnja na to da je uzrok incidenta primjerice nenamjerna greška u radu ili na opremi? Ako se sumnja da se radi o nezakonitom ili zlonamjernom djelovanju, to je potrebno navesti ovdje uz kratko obrazloženje.

Procjena može li incident imati prekogranični utjecaj*

Potrebno je navesti procjenu subjekta može li incident imati prekogranični utjecaj. Ako subjekt smatra da incident može imati prekogranični utjecaj, onda je potrebno navesti i kratko obrazloženje.

Procjena može li incident imati međusektorski utjecaj*

Potrebno je navesti procjenu subjekta može li incident imati međusektorski utjecaj. Ako subjekt smatra da incident može imati međusektorski utjecaj, onda je potrebno navesti i kratko obrazloženje.

Traži li se pomoć CSIRT-a

Potrebno je navesti traži li subjekt pomoć od CSIRT-a u odgovoru na incident, te ako traži, onda je potrebno ukratko navesti za koje aspekte odgovora na incident traži pomoć (npr. potrebna je pomoć u istrazi, potrebne su preporuke koje bi dodatne sigurnosne mjere trebalo implementirati i sl.).

Početna obavijest o značajnom incidentu i Privremeno izvješće o značajnom incidentu

Obrasci za početnu obavijest o značajnom incidentu i privremeno izvješće o značajnom incidentu su isti. Ti obrasci sadrže većinom ista polja kao i obrazac za rano upozorenje o značajnom incidentu, uz sljedeće razlike:

- polje „Po kojim kriterijima je incident značajan“ je sada obavezno, tj. subjekt ga mora popuniti u ovim obrascima,
- polje „Opis osnovnih značajki incidenta“ je zamijenjeno s poljem „Ažurirani opis značajki incidenta i drugih informacija te početna procjena značajnog incidenta“.

Za polja koja su ista kao i u obrascu za rano upozorenje o značajnom incidentu vrijede iste upute, dok su upute za novo/izmijenjeno polje navedene u nastavku.

Ažurirani opis značajki incidenta i drugih informacija te početna procjena značajnog incidenta*

U ovom polju treba navesti trenutno dostupne informacije o incidentu koje nisu obuhvaćene kroz ostala polja. Kako bi se olakšalo strukturirano popunjavanje ovog polja, subjekt može pratiti pitanja navedena u uputama za polje „Opis osnovnih značajki incidenta” ranog upozorenja.

S obzirom na to da se radi o početnoj obavijesti odnosno privremenom izvješću, i dalje se ne očekuje da subjekt ima odgovor na sva navedena pitanja, ali se očekuje da informacije iz ranog upozorenja, odnosno prethodne obavijesti/izvješća, budu nadopunjene s novim saznanjima.

Izvješće o napretku

Obrazac za izvješće o napretku većinom sadrži ista polja kao i obrazac za početnu obavijest o značajnom incidentu, uz sljedeće razlike:

- polje „Ažurirani opis značajki incidenta i drugih informacija te početna procjena značajnog incidenta“ je zamijenjeno s poljem „Ažurirani opis osnovnih značajki incidenta, početne procjene značajnog incidenta i drugih informacija“,
- dodano je polje „Procjena i obrazloženje uzroka koji su doveli do produženog trajanja odgovora na incident uz procjenu kada bi incident mogao biti završen“.

Za polja koja su ista kao i u obrascu za početnu obavijest o značajnom incidentu vrijede iste upute, dok su za nova/izmijenjena polja upute navedene u nastavku.

Ažurirani opis osnovnih značajki incidenta, početne procjene značajnog incidenta i drugih informacija*

U ovom polju treba navesti trenutno dostupne informacije o incidentu koje nisu obuhvaćene kroz ostala polja, s naglaskom na ažuriranje prethodno navedenih informacija (opis osnovnih značajki incidenta, početne procjene značajnog incidenta i drugih informacija) te opis dodatnih sigurnosnih mjera odnosno mjera za ublažavanje rizika koje su primijenjene ili se tek planiraju primijeniti.

Kako bi se olakšalo strukturirano popunjavanje ovog polja, subjekt može pratiti pitanja navedena u uputama za polje „Opis osnovnih značajki incidenta" ranog upozorenja.

Procjena i obrazloženje uzroka koji su doveli do produženog trajanja odgovora na incident uz procjenu kada bi incident mogao biti završen*

Izvješće o napretku se dostavlja umjesto završnog izvješća o značajnom incidentu ako je incident još u tijeku, sukladno uputama u poglavlju „Vrste obavijesti i rokovi za dostavu" Općih smjernica. S obzirom na to da odgovor na incident još nije završen (pa se dostavlja izvješće o napretku umjesto završnog izvješća), potrebno je obrazložiti koji su uzroci doveli do produženog trajanja odgovora na incident te navesti procjenu kada bi incident mogao biti završen.

Završno izvješće o značajnom incidentu

Obrazac za završno izvješće većinom sadrži ista polja kao i obrazac za početnu obavijest o značajnom incidentu, uz sljedeće razlike:

- polje „Ažurirani opis značajki incidenta i drugih informacija te početna procjena značajnog incidenta" je zamijenjeno s poljem „Detaljan opis incidenta i druge informacije",
- dodano je polje „Podaci o prekograničnom učinku incidenta",
- dodano je polje „Podaci o međusektorskom učinku incidenta".

Za polja koja su ista kao i u obrascu za početnu obavijest o značajnom incidentu vrijede iste upute, dok su za nova/izmijenjena polja upute navedene u nastavku.

Detaljan opis incidenta i druge informacije*

U ovom polju treba navesti trenutno dostupne informacije o incidentu koje nisu obuhvaćene kroz ostala polja, uključujući:

- detaljan opis incidenta
- podatke o kibernetičkom napadaču na kojeg se sumnja ili je potvrđen
- podatke o ozbiljnosti i učinku incidenta koji obvezno uključuju opis poremećaja koje je incident izazvao u pružanju usluga, odnosno obavljanju djelatnosti subjekta, trajanju incidenta i broju primatelja usluga na koje je incident utjecao te o možebitnoj kompromitaciji osjetljivih podataka
- primijenjene mjere ublažavanja rizika i mjere ublažavanja rizika čija primjena je u tijeku

- mjere za postizanje više razine kibernetičke sigurnosti koje subjekt planira primijeniti kako bi se minimizirala mogućnost ponavljanja istog ili sličnog incidenta te kako bi se ublažio rizik

Kako bi se olakšalo strukturirano popunjavanje ovog polja, subjekt može pratiti pitanja navedena u uputama za polje „Opis osnovnih značajki incidenta" ranog upozorenja.

Podaci o prekograničnom učinku incidenta

Ako je incident imao prekogranični učinak, ovdje je potrebno navesti dostupne podatke o tom učinku.

Podaci o međusektorskom učinku incidenta

Ako je incident imao međusektorski učinak, ovdje je potrebno navesti dostupne podatke o tom učinku.

Prilog

Obrasci za rano upozorenje, početnu obavijest, privremeno izvješće, izvješće o napretku te završno izvješće o značajnom incidentu dostupni su na sljedećim poveznicama (isti obrasci su dostupni na obje poveznice):

- https://www.ncsc.hr/hr/obrasci-za-prijavu-znacajnih-incidenata
- https://www.cert.hr/zks-incident

Sigurnosno-obavještajna agencija

Nacionalni centar za kibernetičku sigurnost

Savska cesta 39/1, 10000 Zagreb

Republika Hrvatska

Kontakt:

E-mail: info@ncsc.hr

www.ncsc.hr

Hrvatska akademska i istraživačka mreža - CARNET

Sektor Nacionalni CERT

Josipa Marohnića 5, 10000 Zagreb

Republika Hrvatska

Kontakt:

E-mail: ncert@cert.hr

www.cert.hr